

TABLE OF CONTENTS

1 (U) Scope and Purpose	1-1
1.1 (U) Scope	1-1
1.2 (U) Purpose	1-1
 2 (U) General Authorities and Principles.....	2-1
2.1 (U) Authority of the Attorney General's Guidelines for Domestic FBI Operations.....	2-1
2.2 (U) General FBI Authorities under AGG-Dom	2-2
2.2.1 (U) Conduct Investigations and Collect Intelligence and Evidence	2-2
2.2.2 (U) Provide Investigative Assistance	2-2
2.2.3 (U) Conduct Intelligence Analysis and Planning	2-2
2.2.4 (U) Retain and Share Information.....	2-2
2.3 (U) FBI as an Intelligence Agency	2-2
2.4 (U) FBI Lead Investigative Authorities.....	2-3
2.4.1 (U) Introduction.....	2-3
2.4.2 (U) Terrorism and Counterterrorism Investigations	2-3
2.4.3 (U) Counterintelligence and Espionage Investigations	2-8
2.4.4 (U) Criminal Investigations.....	2-9
2.4.5 (U) Authority of an FBI Special Agent.....	2-9
2.5 (U) Status as Internal Guidance	2-10
2.6 (U) Departure from the AGG-Dom (AGG-Dom I.D.3)	2-10
2.6.1 (U) Definition	2-10
2.6.2 (U) Departure from the AGG-Dom in Advance.....	2-10
2.6.3 (U) Emergency Departures from the AGG-Dom	2-10
2.6.4 (U) Records of Departures from the AGG-Dom	2-11
2.7 (U) Departures from the DIOG.....	2-11
2.7.1 (U) Definition	2-11
2.7.2 (U) Departure from the DIOG.....	2-11
2.7.3 (U) Emergency Departures from the DIOG.....	2-11
2.7.4 (U) Records of Departures from the DIOG.....	2-12
2.8 (U) Discovery of Non-compliance with DIOG Requirements after-the-fact.....	2-12
2.8.1 (U) Substantial Non-Compliance with the DIOG	2-12
2.8.2 (U) Documentation of Substantial non-Compliance.....	2-13

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

2.8.3	(U) Reporting Authorities.....	2-14
2.8.4	(U) Role of OIC and OGC.....	2-14
2.8.5	(U) Potential IOB matters involving the reports of Substantial Non-Compliance	2-14
2.8.6	(U) Reporting Non-Compliance with Policy Implementation Guides	2-14
2.8.7	(U) Reporting Non-Compliance with other FBI Policies and Procedures (outside the DIOG).....	2-15
2.9	(U) Other FBI Activities Not Limited by AGG-Dom	2-15
2.10	(U) Use of Classified Investigative Technologies.....	2-15
2.11	(U) Application of AGG-Dom and DIOG	2-15
3	(U) Core Values, Roles, and Responsibilities.....	3-1
3.1	(U) The FBI's Core Values.....	3-1
3.1.1	(U) Compliance.....	3-1
3.2	(U) Investigative Authority, Roles and Responsibility of the Director's Office	3-2
3.2.1	(U) Director's Authority, Roles and Responsibility.....	3-2
3.2.2	(U) Deputy Director's Authority, Roles and Responsibility.....	3-2
3.3	(U) Special Agent/Intelligence Analyst/Task Force Officer (TFO)/Task Force Member (TFM)/Task Force Participant (TFP)/FBI Contractor/Others - Roles and Responsibilities	3-3
3.3.1	(U) Roles and Responsibilities.....	3-3
3.3.1.1	(U) Training.....	3-3
3.3.1.2	(U) Investigative Activity.....	3-3
3.3.1.3	(U) Privacy and Civil Liberties.....	3-3
3.3.1.4	(U) Protect Rights	3-4
3.3.1.5	(U) Compliance	3-4
3.3.1.6	(U) Report Non-Compliance.....	3-4
3.3.1.7	(U) Assist Victims.....	3-4
3.3.1.8	(U) Obtain Approval.....	3-4
3.3.1.9	(U) Attribute Information to Originator in Reports	3-4
3.3.1.10	(U) Serve as Investigation ("Case") Manager	3-4
3.3.1.11	(U) Create and Maintain Records/Files	3-5
3.3.1.12	(U) Index Documents.....	3-5
3.3.1.13	(U) Seek Federal Prosecution	3-5
3.3.1.14	(U) Retain Notes Made During An Investigation.....	3-5
3.3.2	(U) Definitions of Task Force Officer (TFO), Task Force Member (TFM), and Task Force Participant (TFP).....	3-6

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

3.3.2.1	(U) Task Force Officer (TFO).....	3-6
3.3.2.2	(U) Task Force Member (TFM).....	3-6
3.3.2.3	(U) Task Force Participant (TFP) (i.e., Task Force Liaison)	3-6
3.4	(U) Supervisor Roles and Responsibilities.....	3-7
3.4.1	(U) Supervisor Defined	3-7
3.4.2	(U) Supervisor Responsibilities	3-7
3.4.2.1	(U) Approval/Review of Investigative or Collection Activities.....	3-7
3.4.2.2	(U) Oral Authority / Approval	3-7
3.4.2.3	(U) No Self-Approval Rule.....	3-8
3.4.2.4	(U) Ensure Compliance with U.S. Regulations and other Applicable Legal and Policy Requirements.....	3-8
3.4.2.5	(U) Training.....	3-8
3.4.2.6	(U) Protect Civil Liberties and Privacy.....	3-8
3.4.2.7	(U) Report Compliance Concerns	3-9
3.4.2.8	(U) Non-Retaliation Policy	3-9
3.4.2.9	(U) Create and Maintain Records/Files	3-9
3.4.3	(U) Delegation and Succession in the FBI	3-9
3.4.3.1	(U) Delegation	3-9
3.4.3.2	(U) Succession: Acting Supervisory Authority.....	3-10
3.4.3.3	(U) Documentation.....	3-10
3.4.4	(U) File Reviews and Justification Reviews	3-10
3.4.4.1	(U) Overview	3-10
3.4.4.2	(U) Types of Files/Investigations Requiring File Reviews and Justification Reviews.....	3-11
3.4.4.3	(U) Frequency of File Reviews.....	3-11
3.4.4.4	(U) Frequency of Justification Reviews	3-11
3.4.4.5	(U) Delegation of File Reviews	3-11
3.4.4.6	(U) File Review Requirements for Predicated Investigations & Assessments.....	3-12
3.4.4.7	(U) Type 1 & 2 Assessments - Justification Reviews	3-14
3.4.4.8	(U) Type 3, 4, and 6 Assessments - Assessment Review Standards (ARS)	3-14
3.4.4.9	(U) Type 5 Assessments - Assessment Review Standards (ARS).....	3-15
3.4.4.10	(U) Documentation of File Reviews.....	3-15
3.4.4.11	(U) Records Retention	3-16
3.5	(U) Chief Division Counsel (CDC) Roles and Responsibilities.....	3-16
3.6	(U) Office of the General Counsel (OGC) Roles and Responsibilities.....	3-17
3.7	(U) Corporate Policy Office (CPO) Roles and Responsibilities.....	3-18

1.1.1. (U) Information Integrity and Compliance (OIC) Roles and Responsibilities	3-18
1.1.2. (U) Operational Program Manager Roles and Responsibilities	3-19
1.1.3. (U) Assessment Compliance Officer Roles and Responsibilities	3-19
1.1.4. (U) Practice Equivalents - FBI Headquarters (FBIHQ) Approval Levels	3-19
4 (U) Privacy and Civil Liberties, and Least Intrusive Methods	4-1
4.1. (U) Civil Liberties and Privacy	4-1
4.2. (U) Protection of First Amendment Rights	4-4
4.3. (U) Equal Protection under the Law	4-11
4.4. (U) Least Intrusive Method	4-15
5 (U) Assessments	5-1
5.1 (U) Overview and Activities Authorized Prior to Opening an Assessment	5-1
5.1.1 (U) Activities Authorized Prior to Opening an Assessment	5-2
5.1.1.1 (U) Public Information	5-2
5.1.1.2 (U) Records or Information - FBI and DOJ	5-2
5.1.1.3 (U) Records or Information - Other federal, state, local, tribal, or foreign government agency	5-2
5.1.1.4 (U) On-line Services and Resources	5-2
5.1.1.5 (U) Clarifying Interview	5-2
5.1.1.6 (U) Information Voluntarily Provided by Governmental or Private Entities	5-2
5.1.2 (U) Documentation Requirements for Record Checks: (Existing /historical information referred to in section 5.1.1 above)	5-3
5.1.3 (U) Liaison Activities and Tripwires	5-3
5.2 (U) Purpose and Scope	5-3
5.2.1 (U) Scenarios	5-4
5.3 (U) Civil Liberties and Privacy	5-7
5.4 (U) Five Types of Assessments (AGG-Dom, Part II.A.3.)	5-8
5.4.1 (U) Assessment Types	5-8
5.5 (U) Standards for Opening or Approving an Assessment	5-8
5.6 (U) Position Equivalents, Effective Date, Duration, Documentation, Approval, Notice, File Review and Responsible Entity	5-9
5.6.1 (U) Field Office and FBIHQ Position Equivalents	5-9
5.6.2 (U) Effective Date of Assessments	5-9
5.6.3 (U) Assessment Types	5-9

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

3.8	(U) Office of Integrity and Compliance (OIC) Roles and Responsibilities	3-18
3.9	(U) Operational Program Manager Roles and Responsibilities.....	3-19
3.10	(U) Division Compliance Officer Roles and Responsibilities	3-19
3.11	(U) Position Equivalents - FBI Headquarters (FBIHQ) Approval Levels	3-19
4	(U) Privacy and Civil Liberties, and Least Intrusive Methods.....	4-1
4.1	(U) Civil Liberties and Privacy	4-1
4.2	(U) Protection of First Amendment Rights	4-4
4.3	(U) Equal Protection under the Law	4-11
4.4	(U) Least Intrusive Method.....	4-15
5	(U) Assessments	5-1
5.1	(U) Overview and Activities Authorized Prior to Opening an Assessment	5-1
5.1.1	(U) Activities Authorized Prior to Opening an Assessment.....	5-2
5.1.1.1	(U) Public Information.....	5-2
5.1.1.2	(U) Records or Information - FBI and DOJ.....	5-2
5.1.1.3	(U) Records or Information – Other federal, state, local, tribal, or foreign government agency	5-2
5.1.1.4	(U) On-line Services and Resources	5-2
5.1.1.5	(U) Clarifying Interview	5-2
5.1.1.6	(U) Information Voluntarily Provided by Governmental or Private Entities.....	5-2
5.1.2	(U) Documentation Requirements for Record Checks: (Existing /historical information referred to in section 5.1.1 above)	5-3
5.1.3	(U) Liaison Activities and Tripwires	5-3
5.2	(U) Purpose and Scope	5-3
5.2.1	(U) Scenarios.....	5-4
5.3	(U) Civil Liberties and Privacy	5-7
5.4	(U) Five Types of Assessments (AGG-Dom, Part II.A.3.)	5-8
5.4.1	(U) Assessment Types.....	5-8
5.5	(U) Standards for Opening or Approving an Assessment.....	5-8
5.6	(U) Position Equivalents, Effective Date, Duration, Documentation, Approval, Notice, File Review and Responsible Entity.....	5-9
5.6.1	(U) Field Office and FBIHQ Position Equivalents	5-9
5.6.2	(U) Effective Date of Assessments.....	5-9
5.6.3	(U) Assessment Types.....	5-9

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

5.6.3.1	(U) Type 1 & 2 Assessments.....	5-9
5.6.3.2	(U) Type 3 Assessments.....	5-12
5.6.3.3	(U) Type 4 Assessments.....	5-17
5.6.3.4	(U) Type 5 Assessments.....	5-20
5.6.3.5	(U) Type 6 Assessments.....	5-29
5.7	(U) Sensitive Investigative Matters (SIM) in Assessments.....	5-32
5.7.1	(U) SIM Categories in Assessments.....	5-32
5.7.2	(U) Academic Nexus in Assessments	5-33
5.8	(U) Standards for Opening or Approving the Use of an Authorized Investigative Method	5-33
5.9	(U) Authorized Investigative Methods in Assessments.....	5-34
5.9.1	(U) Type 1 through 4 and Type 6 Assessments.....	5-34
5.9.2	(U) Type 5 Assessments	5-34
5.10	(U) Other Investigative Methods Not Authorized During Assessments	5-34
5.11	(U) Intelligence Collection (i.e., Incidental Collection).....	5-34
5.12	(U) Retention and Dissemination of Privacy Act Records	5-35
5.12.1	(U) Marking Closed Assessments That Contain Personal Information.....	5-36
5.12.1.1	(U) Type 1& 2 Assessments	5-36
5.12.1.2	(U) Type 3, 4, and 6 Assessments.....	5-36
5.12.1.3	(U) Type 5 Assessments.....	5-36
5.13	(U) Assessment File Records Management and Retention	5-37
5.14	(U) Other Program Specific Investigation Requirements	5-37
6	(U) Preliminary Investigations	6-1
6.1	(U) Overview	6-1
6.2	(U) Purpose and Scope	6-1
6.3	(U) Civil Liberties and Privacy	6-1
6.4	(U) Legal Authority	6-2
6.4.1	(U) Criminal Investigations.....	6-2
6.4.2	(U) Threats to the National Security	6-2
6.5	(U) Predication	6-3
6.6	(U) Standards for Opening or Approving a Preliminary Investigation	6-3
6.7	(U) Opening Documentation, Approval, Effective Date, Notice, Extension, Pending Inactive Status, Conversion, and File Review.....	6-4
6.7.1	(U) Opening Documentation.....	6-4
6.7.1.1	(U) Approval / Effective Date / Notice.....	6-4

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

6.7.2	(U) Extension	6-5
6.7.2.1	(U) Good Cause.....	6-6
6.7.3	(U) Pending Inactive Status.....	6-6
6.7.4	(U) Conversion to Full Investigation.....	6-6
6.7.5	(U) File Review.....	6-6
6.8	(U) Standards for Opening or Approving the Use of an Authorized Investigative Method in Preliminary Investigations	6-6
6.9	(U) Authorized Investigative Methods in Preliminary Investigations.....	6-7
6.10	(U) Sensitive Investigative Matters (SIM) in Preliminary Investigations	6-8
6.10.1	(U) SIM Categories in Preliminary Investigations	6-8
6.10.2	(U) Academic Nexus in Preliminary Investigations	6-8
6.11	(U) Intelligence Collection (i.e., Incidental Collection).....	6-9
6.12	(U) Standards for Approving the Closing of a Preliminary Investigation	6-9
6.12.1	(U) Standards.....	6-9
6.12.2	(U) Approval Requirements to Close	6-10
6.13	(U) Other Program Specific Investigative Requirements.....	6-10
7	(U) Full Investigations.....	7-1
7.1	(U) Overview	7-1
7.2	(U) Purpose and Scope	7-1
7.3	(U) Civil Liberties and Privacy	7-1
7.4	(U) Legal Authority	7-2
7.4.1	(U) Criminal Investigations.....	7-2
7.4.2	(U) Threats to the National Security	7-3
7.4.3	(U) Foreign Intelligence Collection	7-3
7.5	(U) Predication	7-3
7.6	(U) Standards for Opening or Approving a Full Investigation.....	7-4
7.7	(U) Opening Documentation, Approval, Effective Date, Notice, Pending Inactive Status, File Review, and Letter Head Memorandum.....	7-4
7.7.1	(U) Opening Documentation.....	7-4
7.7.1.1	(U) Approval / Effective Date / Notice.....	7-4
7.7.2	(U) Pending Inactive Status.....	7-6
7.7.3	(U) File Review.....	7-6
7.7.4	(U) Annual Letterhead Memorandum	7-6
7.8	(U) Standards for Opening or Approving the Use of an Authorized Investigative Method in Full Investigations	7-7

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

7.9	(U) Authorized Investigative Methods in Full Investigations	7-7
7.10	(U) Sensitive Investigative Matters (SIM) in Full Investigations	7-8
7.10.1	(U) SIM Categories in Full Investigations	7-8
7.10.2	(U) Academic Nexus in Full Investigations	7-9
7.11	(U) Intelligence Collection (i.e., Incidental Collection)	7-9
7.12	(U) Standards for Approving the Closing of a Full Investigation	7-10
7.12.1	(U) Standards	7-10
7.12.2	(U) Approval Requirements to Close	7-11
7.13	(U) Other Program Specific Investigative Requirements	7-11
8	(U) Enterprise Investigations (EI)	8-1
8.1	(U) Overview	8-1
8.2	(U) Purpose, Scope and Definitions	8-1
8.3	(U) Civil Liberties and Privacy	8-2
8.4	(U) Predication	8-3
8.5	(U) Standards for Opening or Approving an Enterprise Investigation	8-4
8.6	(U) Opening Documentation, Effective Date, Approval, Notice, and File Review	8-4
8.6.1	(U) Opening Documentation	8-4
8.6.2	(U) Effective Date	8-4
8.6.3	(U) Approval Requirements for Opening an Enterprise Investigation	8-5
8.6.3.1	(U) EI Opened by a Field Office with Section Chief Approval	8-5
8.6.3.2	(U) EI Opened by FBIHQ with Section Chief Approval	8-5
8.6.3.3	(U) SIM EI Opened by a Field Office with Special Agent in Charge and Section Chief Approval	8-5
8.6.3.4	(U) SIM EI Opened by FBIHQ with Section Chief Approval	8-5
8.6.4	(U) Notice Requirements	8-6
8.6.5	(U) File Review	8-6
8.7	(U) Authorized Investigative Methods in an Enterprise Investigation	8-7
8.8	(U) Sensitive Investigative Matters (SIM) in Enterprise Investigations	8-7
8.8.1	(U) SIM Categories in Enterprise Investigations	8-7
8.8.2	(U) Academic nexus in Enterprise Investigations	8-7
8.9	(U) Intelligence Collection (i.e., Incidental Collection)	8-8
8.10	(U) Standards for Approving the Closing of an Enterprise Investigation	8-8
8.10.1	(U) Standards	8-8
8.10.2	(U) Approval Requirements to Close	8-9

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

8.11 (U) Other Program Specific Investigative Requirements.....	8-9
9 (U) Foreign Intelligence.....	9-1
9.1 (U) Overview.....	9-1
9.2 (U) Purpose and Scope.....	9-2
9.3 (U) Civil Liberties and Privacy.....	9-3
9.4 (U) Legal Authority.....	9-4
9.5 (U) General Requirements and FBIHQ Standards for Approving the Opening of Positive Foreign Intelligence Investigations.....	9-4
9.6 (U) Opening Documentation, Approval, Effective Date, and File Review.....	9-5
9.7 (U) Standards for Opening or Approving the Use of an Authorized Investigative Method in a Full Positive Foreign Intelligence Investigation.....	9-8
9.8 (U) Authorized Investigative Methods in a Full Positive Foreign Intelligence Investigation.....	9-8
9.9 (U) Investigative Methods Not Authorized During A Full Positive Foreign Intelligence Investigation.....	9-9
9.10 (U) Sensitive Investigative Matters (SIM) in a Full Positive Foreign Intelligence Investigation.....	9-10
9.11 (U) Retention of Information.....	9-11
9.12 (U//FOUO) Standards for Approving the Closing of a Full Positive Foreign Intelligence Investigation.....	9-11
9.13 (U) Other Program Specific Investigation Requirements.....	9-12
10(U//FOUO) Sensitive Investigative Matter (SIM) and Sensitive Operations Review Committee (SORC).....	10-1
10.1 (U) Sensitive Investigative Matters (SIM).....	10-1
10.1.1 (U) Overview.....	10-1
10.1.2 (U) Purpose, Scope, and Definitions.....	10-1
10.1.2.1 (U) Definition of Sensitive Investigative Matters (SIM).....	10-1
10.1.2.2 (U) Definitions/Descriptions of SIM Officials and Entities.....	10-1
10.1.3 (U) Factors to Consider When Opening or Approving an Investigative Activity Involving a SIM.....	10-4
10.1.4 (U) Opening Documentation, Approval, Notice, and Change in SIM Status.....	10-4
10.1.4.1 (U) Review and Approval of SIM Assessments By A Field Office.....	10-4
10.1.4.2 (U) Notice for SIM Assessments by a Field Office.....	10-5
10.1.4.3 (U) Review and Approval of SIM Predicated Investigations by a Field Office.....	10-5

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

10.1.4.4	(U) Notice for SIM Predicated Investigations by a Field Office.....	10-6
10.1.4.5	(U) Review and Approval of SIM Assessments Opened by FBIHQ	10-6
10.1.4.6	(U) Notice Requirements for SIM Assessments by FBIHQ.....	10-7
10.1.4.7	(U) Notice for SIM Predicated Investigations by FBIHQ.....	10-8
10.1.4.8	(U) Change in SIM Status	10-8
10.1.4.9	(U) Closing SIM Investigations	10-9
10.1.5	(U) Distinction Between SIM and Sensitive Circumstance in Undercover Operations.....	10-10
10.1.6	(U) Distinction Between SIM and Sensitive Undisclosed Participation.....	10-10
10.1.6.1	(U) Scenarios.....	10-11
10.2	(U//FOUO) Sensitive Operations Review Committee	10-11
10.2.1	(U) Membership and Staffing.....	10-11
10.2.2	(U) Function.....	10-12
10.2.3	(U) Review and Recommendation	10-12
10.2.3.1	(U) Factors to Consider for Review and Recommendation	10-13
10.2.3.2	(U) Process for Review and Recommendation	10-13
10.2.4	(U) Emergency Authorization.....	10-15
10.2.4.1	(U) Notice/Oversight Function of SORC.....	10-15
10.2.5	(U) Logistics.....	10-16
11	(U) Liaison Activities and Tripwires	11-1
11.1	(U) Overview	11-1
11.2	(U) Purpose and Scope	11-1
11.3	(U) Approval Requirements for Liaison and Tripwires.....	11-1
11.4	(U) Documentation & Records Retention Requirements.....	11-2
12	(U) Assistance to Other Agencies.....	12-1
12.1	(U) Overview	12-1
12.2	(U) Purpose and Scope	12-1
12.2.1	(U) Investigative Assistance	12-1
12.2.2	(U) Technical Assistance	12-2
12.3	(U) Investigative Assistance to Other Agencies - Standards, Approvals and Notice Requirements	12-2
12.3.1	(U) Standards for Providing Investigative Assistance to Other Agencies.....	12-2

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

12.3.2	(U) Authority, Approval and Notice Requirements for Providing Investigative Assistance to Other Agencies	12-3
12.3.2.1	(U) Investigative Assistance to United States Intelligence Community (USIC) Agencies	12-3
12.3.2.2	(U) Investigative Assistance to Other United States Federal Agencies	12-4
12.3.2.3	(U) Investigative Assistance to State, Local and Tribal Agencies	12-6
12.3.2.4	(U) Investigative Assistance to Foreign Agencies	12-10
12.4	(U) Technical Assistance to Other Agencies – Standards, Approvals and Notice Requirements	12-12
12.4.1	(U) Authority	12-13
12.4.2	(U) Approval Requirements	12-13
12.4.2.1	(U) Technical Assistance to USIC Agencies	12-13
12.4.2.2	(U) Technical Assistance to Federal, State, Local and Tribal (Domestic) Agencies Regarding Electronic Surveillance, Equipment, and Facilities	12-13
12.4.2.3	(U) Technical Assistance to Federal, State, Local and Tribal (Domestic) Agencies Involving Equipment or Technologies Other than Electronic Surveillance Equipment	12-14
12.4.2.4	(U) Technical Assistance to Foreign Agencies	12-15
12.5	(U) Documentation Requirements for Investigative or Technical Assistance to Other Agencies	12-16
12.5.1	(U) Documentation Requirements in General	12-16
12.5.2	(U) Documentation Requirements for Investigative Assistance (including Expert Assistance) to Other Agencies (Domestic or Foreign)	12-16
12.5.3	(U) Documentation Requirements for Technical Assistance to Other Agencies (Domestic or Foreign)	12-17
12.6	(U) Dissemination of Information to Other Agencies – Documentation Requirements	12-17
12.7	(U) Records Retention Requirements	12-18
12.7.1	(U) Use of the FD-999	12-18
12.7.2	(U) Uploading the FD-999	12-18
12.7.3	(U) Request for FD-999 Exemption	12-18
12.7.4	(U//FOUO) 343 File Classification - Domestic Police Cooperation Files	12-19
12.7.5	(U//FOUO) 163 File Classification - Foreign Police Cooperation Files	12-19
13(U)	Extraterritorial Provisions	13-1
13.1	(U) Overview	13-1
13.2	(U) Purpose and Scope	13-1
13.3	(U) Joint Venture Doctrine	13-2

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

13.4 (U) Legal Attaché Program	13-2
14(U) Retention and Sharing of Information	14-1
14.1 (U) Purpose and Scope	14-1
14.2 (U) The FBI's Records Retention Plan, and Documentation	14-1
14.2.1 (U) Database or Records System	14-2
14.2.2 (U) Records Management Division Disposition Plan and Retention Schedules.....	14-2
14.3 (U) Information Sharing.....	14-2
14.3.1 (U) Permissive Sharing.....	14-2
14.3.2 (U) Required Sharing.....	14-3
14.4 (U) Information Related to Criminal Matters.....	14-3
14.4.1 (U) Coordinating with Prosecutors.....	14-3
14.4.2 (U) Criminal Matters Outside FBI Jurisdiction.....	14-4
14.4.3 (U) Reporting Criminal Activity of an FBI Employee or CHS	14-4
14.5 (U) Information Related to National Security and Foreign Intelligence Matters.....	14-4
14.5.1 (U) Department of Justice	14-5
14.5.2 (U) The White House	14-6
14.5.3 (U) Congress.....	14-7
14.6 (U) Special Statutory Requirements	14-7
14.7 (U) Threat To Life – Dissemination Of Information	14-8
14.7.1 (U) Overview	14-8
14.7.2 (U//FOUO) Information Received through FISA Surveillance	14-8
14.7.3 (U) Dissemination of Information Concerning Threats against Intended Victims (Persons).....	14-8
14.7.4 (U//FOUO) Dissemination of Information Concerning Threats, Possible Violence or Demonstrations Against Foreign Establishments or Officials in the United States...	14-11
14.7.5 (U) Dissemination of Information Concerning Threats against the President and Other Designated Officials	14-11
15(U) Intelligence Analysis and Planning	15-1
15.1 (U) Overview	15-1
15.2 (U) Purpose and Scope	15-1
15.2.1 (U) Functions Authorized	15-1
15.2.2 (U) Integration of Intelligence Activities	15-2

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

15.2.3	(U) Analysis and Planning Not Requiring the Opening of an Assessment (See DIOG Section 5)	15-2
15.3	(U) Civil Liberties and Privacy	15-2
15.4	(U) Legal Authority	15-2
15.5	(U) Intelligence Analysis and Planning – Requiring a Type 4 Assessment	15-3
15.6	(U) Authorized Activities in Intelligence Analysis and Planning	15-3
15.6.1	(U) Strategic Intelligence Analysis	15-3
16	(U) Undisclosed Participation (UDP)	16-1
16.1	(U) Overview	16-1
16.1.1	(U) Authorities	16-1
16.1.2	(U) Mitigation of Risk	16-2
16.1.3	(U) Sensitive UDP defined	16-2
16.1.4	(U) Non-sensitive UDP defined	16-2
16.1.5	(U) Type of Activity	16-2
16.2	(U) Purpose, Scope, and Definitions	16-2
16.2.1	(U) Organization	16-2
16.2.2	(U) Legitimate Organization	16-3
16.2.3	(U) Participation	16-3
16.2.3.1	(U) Undisclosed Participation	16-4
16.2.3.2	(U//FOUO) Influencing the Activities of the Organization	16-5
16.2.3.3	(U//FOUO) Influencing the exercise of First Amendment rights	16-5
16.2.3.4	(U) Appropriate Official	16-5
16.2.3.5	(U) Sensitive Undisclosed Participation	16-5
16.2.3.6	(U) Already a Member of the Organization or a Participant in its Activities	16-6
16.3	(U) Requirements for Approval	16-6
16.3.1	(U) General Requirements	16-6
16.3.1.1	(U) Undercover Activity	16-6
16.3.1.2	(U) Concurrent Approval	16-6
16.3.1.3	(U) Delegation and “Acting” Status	16-7
16.3.1.4	(U) Specific Requirements for General Undisclosed Participation (Non-sensitive UDP)	16-7
16.3.1.5	(U) Specific Requirements for Sensitive Undisclosed Participation (Sensitive UDP)	16-8
16.4	(U) Supervisory Approval Not Required	16-9
16.5	(U) Standards for Review and Approval	16-10

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

16.6 (U) Requests for Approval of Undisclosed Participation	16-10
16.7 (U) Duration	16-11
16.8 (U//FOUO) Sensitive Operations Review Committee (SORC)	16-12
16.8.1 (U//FOUO) SORC Notification	16-12
16.8.2 (U//FOUO) SORC Review	16-12
16.9 (U) FBIHQ Approval Process of UDP Requests	16-12
16.9.1 (U) Submitting the UDP request to FBIHQ	16-12
16.9.2 (U//FOUO) Assessments – CHSs tasked to join sensitive organizations and obtain insider information	16-13
16.9.3 (U//FOUO) Predicated Investigations – UDP Requests intended to or which may influence the activities of an organization or the exercise of First Amendment rights by its members	16-13
16.9.4 (U//FOUO) Procedures for approving emergency UDP requests that otherwise require FBIHQ approval	16-14
16.10 (U) UDP Examples	16-15
 17(U) Otherwise Illegal Activity (OIA)	17-1
17.1 (U) Overview	17-1
17.2 (U) Purpose and Scope	17-1
17.3 (U//FOUO) OIA in Undercover Activity	17-1
17.4 (U//FOUO) OIA by a Confidential Human Source (CHS)	17-2
17.5 (U//FOUO) Approval of OIA by a Special Agent in Charge (SAC) – Not including material Support of Terrorism	17-2
17.6 (U//FOUO) OIA Related to Material Support of Terrorism in National Security Investigations	17-4
17.7 (U//FOUO) Standards for Review and Approval of OIA	17-4
17.8 (U) OIA not authorized	17-4
17.9 (U) Emergency Situations	17-5
 18(U) Investigative Methods	18-1
18.1 (U) Overview	18-1
18.1.1 (U) Investigative Methods Listed by Sub-Section Number	18-1
18.1.2 (U) Investigative Methods Listed by Name (Alphabetized)	18-2
18.1.3 (U) General Overview	18-3
18.2 (U) Least Intrusive Method	18-3

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.3 (U) Particular Investigative Methods.....	18-4
18.3.1 (U) Use of Criminal Investigative Methods in National Security Investigations.....	18-4
18.4 (U) Information or Evidence Obtained in Assessments and Predicated Investigations.....	18-4
18.5 (U) Authorized Investigative Methods in Assessments.....	18-5
18.5.1 (U) Investigative Method: Public Information ("Publicly Available Information").....	18-7
18.5.1.1 (U) Scope.....	18-7
18.5.1.2 (U) Application.....	18-8
18.5.1.3 (U) Approval.....	18-8
18.5.1.3.1 (U//FOUO) Special Rules: "Special Rule for Religious Services" and "Special Rule for Other Sensitive Organizations".....	18-8
18.5.1.4 (U) Use/Dissemination.....	18-8
18.5.2 (U) Investigative Method: Records or Information – FBI and Department of Justice (DOJ).....	18-9
18.5.2.1 (U) Scope.....	18-9
18.5.2.2 (U) Application.....	18-9
18.5.2.3 (U) Approval.....	18-9
18.5.2.4 (U) Pattern-Based Data Mining.....	18-9
18.5.2.5 (U) Use/Dissemination.....	18-10
18.5.3 (U) Investigative Method: Records or Information – Other Federal, State, Local, Tribal, or Foreign Government Agency.....	18-11
18.5.3.1 (U) Scope.....	18-11
18.5.3.2 (U) Application.....	18-11
18.5.3.4 (U) Use/Dissemination.....	18-12
18.5.4 (U) Investigative Method: On-Line Services and Resources.....	18-13
18.5.4.1 (U) Scope.....	18-13
18.5.4.2 (U) Application.....	18-13
18.5.4.3 (U) Approval.....	18-13
18.5.4.4 (U) Use/Dissemination.....	18-13
18.5.5 (U) Investigative Method: CHS Use and Recruitment.....	18-15
18.5.5.1 (U) Scope.....	18-15
18.5.5.2 (U) Application.....	18-15
18.5.5.3 (U) Approvals.....	18-15
18.5.5.4 (U) Use/Dissemination.....	18-17
18.5.6 (U) Investigative Method: Interview or Request Information from the Public or Private Entities.....	18-19
18.5.6.1 (U) Scope.....	18-19

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.3 (U) Particular Investigative Methods	18-4
18.3.1 (U) Use of Criminal Investigative Methods in National Security Investigations	18-4
18.4 (U) Information or Evidence Obtained in Assessments and Predicated Investigations	18-4
18.5 (U) Authorized Investigative Methods in Assessments	18-5
18.5.1 (U) Investigative Method: Public Information ("Publicly Available Information")	18-7
18.5.1.1 (U) Scope	18-7
18.5.1.2 (U) Application	18-8
18.5.1.3 (U) Approval	18-8
18.5.1.3.1 (U//FOUO) Special Rules: "Special Rule for Religious Services" and "Special Rule for Other Sensitive Organizations"	18-8
18.5.1.4 (U) Use/Dissemination	18-8
18.5.2 (U) Investigative Method: Records or Information – FBI and Department of Justice (DOJ)	18-9
18.5.2.1 (U) Scope	18-9
18.5.2.2 (U) Application	18-9
18.5.2.3 (U) Approval	18-9
18.5.2.4 (U) Pattern-Based Data Mining	18-9
18.5.2.5 (U) Use/Dissemination	18-10
18.5.3 (U) Investigative Method: Records or Information – Other Federal, State, Local, Tribal, or Foreign Government Agency	18-11
18.5.3.1 (U) Scope	18-11
18.5.3.2 (U) Application	18-11
18.5.3.4 (U) Use/Dissemination	18-12
18.5.4 (U) Investigative Method: On-Line Services and Resources	18-13
18.5.4.1 (U) Scope	18-13
18.5.4.2 (U) Application	18-13
18.5.4.3 (U) Approval	18-13
18.5.4.4 (U) Use/Dissemination	18-13
18.5.5 (U) Investigative Method: CHS Use and Recruitment	18-15
18.5.5.1 (U) Scope	18-15
18.5.5.2 (U) Application	18-15
18.5.5.3 (U) Approvals	18-15
18.5.5.4 (U) Use/Dissemination	18-17
18.5.6 (U) Investigative Method: Interview or Request Information from the Public or Private Entities	18-19
18.5.6.1 (U) Scope	18-19

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.5.6.2	(U) Application.....	18-19
18.5.6.3	(U) Voluntariness.....	18-19
18.5.6.4	(U) Approval / Procedures	18-20
18.5.6.4.1	(U) Custodial Interviews.....	18-20
18.5.6.4.2	(U//FOUO) Miranda Warnings for Suspects in Custody Overseas.....	18-23
18.5.6.4.3	(U) Constitutional Rights to Silence and Counsel under Miranda.....	18-23
18.5.6.4.4	(U) Sixth Amendment Right to Counsel.....	18-24
18.5.6.4.5	(U) Contact with Represented Persons.....	18-25
18.5.6.4.6	(U) Members of the United States Congress and their Staffs	18-25
18.5.6.4.7	(U) White House Personnel.....	18-25
18.5.6.4.8	(U) Members of the News Media.....	18-26
18.5.6.4.9	(U) During an Assessment - Requesting Information without Revealing FBI Affiliation or the True Purpose of a Request.....	18-27
18.5.6.4.10	(U) Consultation and Discussion	18-28
18.5.6.4.11	(U) Examples	18-28
18.5.6.4.12	(U//FOUO) Predicated Investigations - Requesting Information without Revealing FBI Affiliation or the True Purpose of a Request	18-31
18.5.6.4.13	(U) Interviews of Juveniles	18-31
18.5.6.4.14	(U) Interviews of Juveniles After Arrest.....	18-32
18.5.6.4.15	(U) Documentation	18-33
18.5.6.4.16	(U) Electronic Recording of Interviews.....	18-34
18.5.6.4.17	(U) Interviews Relating to Closed Files	18-35
18.5.6.4.18	(U) FBIHQ Operational Division Requirements.....	18-35
18.5.6.5	(U) Use/Dissemination.....	18-36
18.5.7	(U) Investigative Method: Information Voluntarily Provided by Governmental or Private Entities.....	18-37
18.5.7.1	(U) Scope	18-37
18.5.7.2	(U) Application.....	18-37
18.5.7.3	(U) Approval	18-37
18.5.7.4	(U) Use/Dissemination.....	18-37
18.5.8	(U) Investigative Method: Physical Surveillance (not requiring a court order).....	18-39
18.5.8.1	(U) Scope	18-39
18.5.8.2	(U) Application.....	18-40
18.5.8.3	(U) Approval	18-40
18.5.8.3.1	(U//FOUO) Standards for Opening or Approving Physical Surveillance During an Assessment	18-40
18.5.8.3.2	(U//FOUO) 72-Hour Period for Assessments.....	18-40
18.5.8.3.3	(U//FOUO) Mobile Surveillance Team (MST) or Mobile Surveillance Team – Armed (MST-A)	18-41
18.5.8.3.4	(U) Aviation Resources.....	18-41

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.5.8.4	(U) Other Physical Surveillance	18-41
18.5.8.5	(U) Maintain a "Surveillance Log" during Physical Surveillance	18-41
18.5.8.6	(U) Use/Dissemination	18-41
18.5.9	(U) Investigative Method: Grand Jury Subpoenas – for telephone or electronic mail subscriber information only (in Type 1 & 2 Assessments)	18-42
18.5.9.1	(U) Scope	18-42
18.5.9.2	(U) Application	18-42
18.5.9.3	(U) Approval	18-42
18.5.9.4	(U) Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701-2712)	18-42
18.5.9.5	(U) Use/Dissemination	18-42
18.6	(U) Authorized Investigative Methods in Preliminary Investigations	18-47
18.6.1	(U) Investigative Method: Consensual Monitoring of Communications, including Electronic Communications	18-49
18.6.1.1	(U) Summary	18-49
18.6.1.2	(U) Application	18-49
18.6.1.3	(U) Legal Authority	18-49
18.6.1.4	(U) Definition of Investigative Method	18-49
18.6.1.5	(U) Standards and Approval Requirements for Consensual Monitoring	18-51
18.6.1.5.1	(U) General Approval Requirements	18-51
18.6.1.6	(U) Consensual Monitoring Situations Requiring Additional Approval	18-53
18.6.1.6.1	(U) Party Located Outside the United States	18-53
18.6.1.6.2	(U) Consent of More than One Party Required for Consensual Monitoring	18-54
18.6.1.6.3	(U) Sensitive Monitoring Circumstance	18-54
18.6.1.7	(U) Duration of Approval	18-57
18.6.1.8	(U) Specific Procedures	18-57
18.6.1.8.1	(U) Documenting Consent to Monitor/Record	18-57
18.6.1.8.2	(U) Documenting Approval	18-58
18.6.1.8.3	(U) Retention of Consensually Monitored Communications	18-58
18.6.1.8.4	(U) Multiple Communications	18-58
18.6.1.8.5	(U) Investigation Specific Approval	18-58
18.6.1.9	(U) Compliance and Monitoring	18-58
18.6.2	(U) Investigative Method: Intercepting the Communications of a Computer Trespasser	18-59
18.6.2.1	(U) Summary	18-59
18.6.2.2	(U) Application	18-59
18.6.2.3	(U) Legal Authority	18-59
18.6.2.4	(U) Definition of the Communications of a Computer Trespasser	18-59

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.5.8.4	(U) Other Physical Surveillance	18-43
18.5.8.5	(U) Maintain a "Surveillance Log" during Physical Surveillance.....	18-43
18.5.8.6	(U) Use/Dissemination.....	18-43
18.5.9	(U) Investigative Method: Grand Jury Subpoenas – for telephone or electronic mail subscriber information only (in Type 1 & 2 Assessments)	18-45
18.5.9.1	(U) Scope	18-45
18.5.9.2	(U) Application.....	18-45
18.5.9.3	(U) Approval	18-45
18.5.9.4	(U) Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701-2712) ...	18-45
18.5.9.5	(U) Use/Dissemination.....	18-46
18.6	(U) Authorized Investigative Methods in Preliminary Investigations.....	18-47
18.6.1	(U) Investigative Method: Consensual Monitoring of Communications, including Electronic Communications.....	18-49
18.6.1.1	(U) Summary.....	18-49
18.6.1.2	(U) Application.....	18-49
18.6.1.3	(U) Legal Authority.....	18-49
18.6.1.4	(U) Definition of Investigative Method	18-49
18.6.1.5	(U) Standards and Approval Requirements for Consensual Monitoring.....	18-51
18.6.1.5.1	(U) General Approval Requirements.....	18-51
18.6.1.6	(U) Consensual Monitoring Situations Requiring Additional Approval.....	18-53
18.6.1.6.1	(U) Party Located Outside the United States.....	18-53
18.6.1.6.2	(U) Consent of More than One Party Required for Consensual Monitoring.....	18-54
18.6.1.6.3	(U) Sensitive Monitoring Circumstance	18-54
18.6.1.7	(U) Duration of Approval.....	18-57
18.6.1.8	(U) Specific Procedures	18-57
18.6.1.8.1	(U) Documenting Consent to Monitor/Record.....	18-57
18.6.1.8.2	(U) Documenting Approval	18-58
18.6.1.8.3	(U) Retention of Consensually Monitored Communications	18-58
18.6.1.8.4	(U) Multiple Communications	18-58
18.6.1.8.5	(U) Investigation Specific Approval	18-58
18.6.1.9	(U) Compliance and Monitoring	18-58
18.6.2	(U) Investigative Method: Intercepting the Communications of a Computer Trespasser.....	18-59
18.6.2.1	(U) Summary.....	18-59
18.6.2.2	(U) Application.....	18-59
18.6.2.3	(U) Legal Authority.....	18-59
18.6.2.4	(U) Definition of the Communications of a Computer Trespasser	18-59

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.6.2.5	(U//FOUO) Use and Approval Requirements for Intercepting the Communications of a Computer Trespasser.....	18-61
18.6.2.5.1	(U) General Approval Requirements.....	18-61
18.6.2.6	(U) Duration of Approval for Intercepting the Communications of a Computer Trespasser.....	18-63
18.6.2.7	(U) Specific Procedures for Intercepting the Communications of a Computer Trespasser.....	18-63
18.6.2.7.1	(U) Documenting Authorization to Intercept	18-63
18.6.2.7.2	(U) Acquiring Only the Trespasser Communications.....	18-63
18.6.2.7.3	(U) Reviewing the Accuracy of the Interception	18-64
18.6.2.7.4	(U) Reviewing the Relevancy of the Interception	18-64
18.6.2.7.5	(U) Duration of Approval.....	18-65
18.6.2.7.6	(U) ELSUR Requirements	18-65
18.6.2.7.7	(U) Multiple Communications	18-65
18.6.2.7.8	(U) Investigation Specific Approval.....	18-65
18.6.2.8	(U) Compliance and Monitoring	18-65
18.6.3	(U) Investigative Method: Closed-Circuit Television/Video Surveillance, Direction Finders, and other Monitoring Devices	18-67
18.6.3.1	(U) Summary.....	18-67
18.6.3.2	(U) Application.....	18-67
18.6.3.3	(U) Legal Authority.....	18-67
18.6.3.4	(U) Definition of Investigative Method	18-67
18.6.3.5	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method.....	18-68
18.6.3.6	(U) Duration of Approval.....	18-68
18.6.3.7	(U) Specific Procedures.....	18-68
18.6.3.8	(U) CCTV/Video Surveillance where there is a Reasonable Expectation of Privacy in the area to be viewed or for the installation of the equipment.....	18-69
18.6.3.9	(U) Compliance and Monitoring.....	18-69
18.6.4	(U) Investigative Method: Administrative Subpoenas (compulsory process)	18-71
18.6.4.1	(U) Overview of Compulsory Process.....	18-71
18.6.4.2	(U) Application.....	18-71
18.6.4.3	(U) Administrative Subpoenas	18-71
18.6.4.3.1	(U) Summary	18-71
18.6.4.3.2	(U) Legal Authority and Delegation.....	18-72
18.6.4.3.3	(U) Approval Requirements	18-74
18.6.4.3.4	(U) Limitations on Use of Administrative Subpoenas	18-75
18.6.4.3.5	(U) Compliance/Monitoring.....	18-78
18.6.5	(U) Investigative Method: Grand Jury Subpoenas (compulsory process)	18-81

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.6.5.1	(U) Overview of Compulsory Process.....	18-81
18.6.5.2	(U) Application.....	18-81
18.6.5.3	(U) Federal Grand Jury Subpoena.....	18-81
18.6.5.3.1	(U) Legal Authorities.....	18-81
18.6.5.3.2	(U) Scope.....	18-82
18.6.5.3.3	(U) Approval Requirements.....	18-82
18.6.5.3.4	(U) Duration of Approval.....	18-82
18.6.5.3.5	(U) Specific Procedures.....	18-82
18.6.5.3.6	(U) Notice and Reporting Requirements.....	18-83
18.6.5.3.7	(U) Grand Jury Proceedings—Generally.....	18-83
18.6.6	(U) Investigative Method: National Security Letter (compulsory process).....	18-93
18.6.6.1	(U) Overview of Compulsory Process.....	18-93
18.6.6.2	(U) Application.....	18-93
18.6.6.3	(U) National Security Letters.....	18-93
18.6.6.3.1	(U) Legal Authority.....	18-93
18.6.6.3.2	(U) Definition of Method.....	18-94
18.6.6.3.3	(U) Approval Requirements.....	18-94
18.6.6.3.4	(U) Standards for Issuing NSLs.....	18-95
18.6.6.3.5	(U) Special Procedures for Requesting Communication Subscriber Information.....	18-96
18.6.6.3.6	(U) Duration of Approval.....	18-96
18.6.6.3.7	(U) Specific Procedures.....	18-96
18.6.6.3.8	(U) Notice and Reporting Requirements.....	18-100
18.6.6.3.9	(U) Receipt of NSL Information.....	18-100
18.6.6.3.10	(U) Electronic Service and Electronic Returns of NSLs.....	18-102
18.6.6.3.11	(U) Dissemination of NSL Material.....	18-103
18.6.6.3.12	(U) Special Procedures for Handling Right to Financial Privacy Act Information.....	18-103
18.6.6.3.13	(U) Payment for NSL-Derived Information.....	18-104
18.6.7	(U) Investigative Method: FISA Order for Business Records (compulsory process).....	18-105
18.6.7.1	(U) Overview of Compulsory Process.....	18-105
18.6.7.2	(U) Application.....	18-105
18.6.7.3	(U) Business Records Under FISA.....	18-105
18.6.7.3.1	(U) Legal Authority.....	18-105
18.6.7.3.2	(U) Definition of Method.....	18-105
18.6.7.3.3	(U) Approval Requirements.....	18-106
18.6.7.3.4	(U) Duration of Court Approval.....	18-106
18.6.7.3.5	(U) Notice and Reporting Requirements.....	18-106
18.6.7.3.6	(U) Compliance Requirements.....	18-106

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.6.7.3.7 (U) FISA Overcollection.....	18-106
18.6.8 (U) Investigative Method: Stored Wire or Electronic Communications and Transactional Records.....	18-107
18.6.8.1 (U) Summary.....	18-107
18.6.8.2 (U) Application.....	18-107
18.6.8.2.1 (U) Stored Data.....	18-107
18.6.8.2.2 (U) Legal Process.....	18-108
18.6.8.2.3 (U) Retrieval.....	18-108
18.6.8.2.4 (U) Basic Subscriber Information.....	18-108
18.6.8.2.5 (U) Preservation of Stored Data.....	18-108
18.6.8.2.6 (U) Cost reimbursement.....	18-109
18.6.8.3 (U) Legal Authority.....	18-109
18.6.8.4 (U) ECPA Disclosures.....	18-109
18.6.8.4.1 (U) Definitions.....	18-110
18.6.8.4.2 (U) Compelled Disclosure.....	18-110
18.6.8.4.3 (U) Voluntary Disclosure.....	18-116
18.6.8.5 (U) Voluntary Emergency Disclosure.....	18-119
18.6.8.5.1 (U) Scope.....	18-119
18.6.8.5.2 (U) Duration of Approval.....	18-120
18.6.8.5.3 (U) Specific Procedures.....	18-120
18.6.8.5.4 (U) Cost Reimbursement.....	18-121
18.6.8.5.5 (U) Notice and Reporting Requirements.....	18-121
18.6.8.5.6 (U) Reporting Voluntary Emergency disclosures.....	18-121
18.6.8.5.7 (U) Roles/Responsibilities.....	18-121
18.6.8.6 (U) Other Applicable Policies.....	18-122
18.6.9 (U) Investigative Method: Pen Registers and Trap/Trace Devices (PR/TT). 18-123	
18.6.9.1 (U) Summary.....	18-123
18.6.9.2 (U) Application.....	18-123
18.6.9.3 (U) Legal Authority.....	18-123
18.6.9.4 (U) Definition of Investigative Method.....	18-123
18.6.9.5 (U) Standards for Use and Approval Requirements for Investigative Method..	18-123
18.6.9.5.1 (U) Pen Register/Trap and Trace under FISA.....	18-123
18.6.9.5.2 (U) Criminal Pen Register/Trap and Trace under Title 18.....	18-125
18.6.9.6 (U) Duration of Approval.....	18-127
18.6.9.7 (U) Specific Procedures.....	18-127
18.6.9.8 (U) Use of FISA Derived Information in Other Proceedings.....	18-128
18.6.9.9 (U) Congressional Notice and Reporting Requirements.....	18-128
18.6.9.9.1 (U) Criminal Pen Register/Trap and Trace- Annual Report.....	18-128

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.6.9.9.2 (U) National Security Pen Registers and Trap and Trace – Semi-Annual	18-129
18.6.9.10 (U) Post Cut-Through Dialed Digits (PCTDD)	18-129
18.6.9.10.1 (U) Overview	18-129
18.6.9.10.2 (U) Collection of PCTDD.....	18-130
18.6.9.10.3 (U) Use of PCTDD.....	18-130
18.6.9.10.4 (U) What constitutes PCTDD content.....	18-131
18.6.9.11 (U//FOUO) Cell Site Simulators/Digital Analyzers/Wireless Intercept Tracking Technology	18-132
18.6.9.11.1 (U//FOUO) To Locate a Known Phone Number	18-132
18.6.9.11.2 (U//FOUO) To Identify an Unknown Target Phone Number	18-133
18.6.9.11.3 (U) PR/TT Order Language	18-134
18.6.10 (U) Investigative Method: Mail Covers.....	18-135
18.6.10.1 (U) Summary.....	18-135
18.6.10.2 (U) Application.....	18-135
18.6.10.3 (U) Legal Authority.....	18-135
18.6.10.4 (U) Definition of Investigative Method	18-135
18.6.10.5 (U) Standard for Use and Approval Requirements for Investigative Method	18-136
18.6.10.6 (U) Duration of Approval	18-138
18.6.10.7 (U) Storage of Mail Cover Information.....	18-138
18.6.10.8 (U) Return of Mail Cover Information to USPS	18-139
18.6.10.9 (U) Compliance and Monitoring	18-139
18.6.11 (U) Investigative Method: Polygraph Examinations	18-141
18.6.11.1 (U) Summary.....	18-141
18.6.11.2 (U) Application.....	18-141
18.6.11.3 (U) Legal Authority.....	18-141
18.6.11.4 (U) Standards for Use and Approval Requirements for Investigative Method ..	18-141
18.6.11.5 (U) Duration of Approval.....	18-141
18.6.11.6 (U) Specific Procedures	18-142
18.6.11.7 (U) Compliance and Monitoring	18-142
18.6.12 (U) Investigative Method: Trash Covers (Searches that Do Not Require a Warrant or Court Order).....	18-143
18.6.12.1 (U) Summary.....	18-143
18.6.12.2 (U) Application.....	18-143
18.6.12.3 (U) Legal Authority.....	18-143
18.6.12.4 (U) Definition of Investigative Method	18-143
18.6.12.4.1 (U) Distinction between "Trash Covers" and Searches of Abandoned Property or Trash	18-143
18.6.12.4.2 (U) Determination of an Area of Curtilage Around a Home.....	18-144

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.6.12.5 (U) Standards for Use and Approval Requirements for Investigative Method ..	18-144
18.6.13 (U) Investigative Method: Undercover Operations	18-145
18.6.13.1 (U) Summary.....	18-145
18.6.13.2 (U) Legal Authority.....	18-145
18.6.13.3 (U) Definition of Investigative Method	18-145
18.6.13.3.1 (U) Distinction Between Sensitive Circumstance and Sensitive Investigative Matter	18-146
18.6.13.4 (U//FOUO) Standards for Use and Approval Requirements for Investigative Method.....	18-146
18.6.13.4.1 (U) Standards for Use of Investigative Method	18-146
18.6.13.4.2 (U//FOUO) Approval Requirements for UCOs (investigations of violations of federal criminal law that do not concern threats to national security or foreign intelligence)	18-146
18.6.13.4.3 (U//FOUO) Approval Requirements for UCOs (investigations of violations that concern threats to national security or foreign intelligence)	18-147
18.6.13.5 (U) Duration of Approval	18-148
18.6.13.6 (U) Additional Guidance.....	18-148
18.6.13.7 (U) Compliance and Monitoring, and Reporting Requirements	18-148
18.7 (U) Authorized Investigative Methods in Full Investigations	18-149
18.7.1 (U) Investigative Method: Searches – With a Warrant or Court Order (reasonable expectation of privacy).....	18-151
18.7.1.1 (U) Summary.....	18-151
18.7.1.2 (U) Legal Authority.....	18-151
18.7.1.3 (U) Definition of Investigative Method	18-152
18.7.1.3.1 (U) Requirement for Reasonableness.....	18-152
18.7.1.3.2 (U) Reasonable Expectation of Privacy	18-152
18.7.1.3.3 (U) Issuance of Search Warrant.....	18-152
18.7.1.3.4 (U) Property or Persons That May be Seized with a Warrant	18-153
18.7.1.4 (U) Approval Requirements for Investigative Method.....	18-157
18.7.1.5 (U) Duration of Approval.....	18-157
18.7.1.6 (U) Specific Procedures	18-157
18.7.1.6.1 (U) Obtaining a Warrant under FRCP Rule 41.....	18-157
18.7.1.6.2 (U) Obtaining a FISA Warrant	18-160
18.7.2 (U) Investigative Method: Electronic Surveillance – Title III.....	18-165
18.7.2.1 (U) Summary.....	18-165
18.7.2.2 (U) Legal Authority.....	18-165
18.7.2.3 (U) Definition of Investigative Method	18-165
18.7.2.4 (U) Title III Generally	18-165
18.7.2.5 (U) Standards for Use and Approval Requirements for Non-Sensitive Title IIIs.....	18-166

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.7.2.6	(U) Standards for Use and Approval Requirements for Sensitive Title IIIs.....	18-166
18.7.2.7	(U) Procedures For Emergency Title III Interceptions	18-167
18.7.2.7.1	(U) Obtaining Emergency Authorization	18-168
18.7.2.7.2	(U) Post-Emergency Authorization.....	18-169
18.7.2.8	(U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy	18-170
18.7.2.9	(U) Duration of Approval for Title III.....	18-171
18.7.2.10	(U) Specific Procedures for Title III Affidavits.....	18-171
18.7.2.11	(U) Dispute Resolution for Title III Applications	18-172
18.7.2.12	(U) Notice and Reporting Requirements – Title III.....	18-172
18.7.3	(U) Investigative Method: Electronic Surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information)	18-175
18.7.3.1	(U) Summary.....	18-175
18.7.3.2	(U) Foreign Intelligence Surveillance Act (FISA)	18-175
18.7.3.2.1	(U) Legal Authority	18-175
18.7.3.2.2	(U) Definition of Investigative Method	18-175
18.7.3.2.3	(U) Standards for Use and Approval Requirements for FISA.....	18-176
18.7.3.2.4	(U) Duration of Approval for FISA.....	18-177
18.7.3.2.5	(U//FOUO) Specific Procedures for FISA	18-177
18.7.3.2.6	(U) Notice and Reporting Requirements for FISA.....	18-179
18.7.3.2.7	(U) Compliance and Monitoring for FISA	18-179
18.7.3.2.8	(U) Special Circumstances for FISA.....	18-180
18.7.3.2.9	(U) FISA Overcollection.....	18-180
18.7.3.2.10	(U) Other Applicable Policies.....	18-180
18.7.3.3	(U) FISA Title VII (acquisition of foreign intelligence information)	18-180
18.7.3.3.1	(U) Summary	18-180
18.7.3.3.2	(U) Legal Authority	18-180
18.7.3.3.3	(U) Definition of Investigative Method.....	18-180
18.7.3.3.4	(U//FOUO) Standards for Use and Approval Requirements for Investigative Method	18-181
18.7.3.3.5	(U) Duration of Approval.....	18-181
18.7.3.3.6	(U//FOUO) Specific Collection Procedures for Title VII.....	18-181
19(U)	Arrest Procedure Policy	19-1
19.1	(U) Arrest Warrants.....	19-1
19.1.1	(U) Complaints	19-1
19.1.2	(U) Arrest Warrants	19-1
19.1.3	(U) Jurisdiction.....	19-1
19.1.4	(U) Person to be Arrested.....	19-1

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

19.2.1	(U) Policy	19-2
19.2.2	(U) Prompt Execution.....	19-2
19.2.3	(U) Arrest Plans.....	19-2
19.2.4	(U) Joint Arrests.....	19-3
19.2.5	(U) Possession and Display of Warrant	19-3
19.3	(U) Arrest without Warrant	19-3
19.3.1	(U) Federal Crimes.....	19-3
19.3.2	(U) Notification to U.S. Attorney	19-3
19.3.3	(U) Non-Federal Crimes	19-3
19.3.4	(U) Adherence to FBI Policy.....	19-4
19.4	(U) Prompt Appearance before Magistrate	19-4
19.4.1	(U) Definition of Unnecessary Delay	19-5
19.4.2	(U) Effect of Unnecessary Delay.....	19-5
19.4.3	(U) Necessary Delay	19-6
19.4.4	(U) Initial Processing	19-6
19.4.5	(U) Collection of DNA after Arrest or Detention	19-6
19.5	(U) Use of Force.....	19-7
19.5.1	(U) Identification	19-7
19.5.2	(U) Physical Force.....	19-7
19.5.3	(U) Restraining Devices.....	19-7
19.5.4	(U) Pregnant Arrestees	19-7
19.6	(U) Manner of Entry.....	19-7
19.6.1	(U) Knock and Announce	19-7
19.6.2	(U) Suspect's Premises.....	19-8
19.6.3	(U) Third Party Premises	19-8
19.6.4	(U) Exigent Circumstances	19-8
19.7	(U) Search Incident to Arrest.....	19-8
19.7.1	(U) Prerequisite: Lawful Arrest.....	19-9
19.7.2	(U) Scope and Timing Requirement.....	19-9
19.7.3	(U) Inventory of Personal Property.....	19-10
19.8	(U) Medical Attention for Arrestees.....	19-10
19.9	(U) Arrest of Foreign Nationals	19-10
19.9.1	(U) Requirements Pertaining to Foreign Nationals	19-10
19.9.2	(U) Steps to Follow When a Foreign National is Arrested or Detained.....	19-11
19.9.3	(U) Suggested Statements to Arrested or Detained Foreign Nationals	19-13
19.9.4	(U) Diplomatic Immunity.....	19-13

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

19.10 (U) Arrest of News Media Members	19-14
19.11 (U) Arrest of Armed Forces Personnel	19-14
19.12 (U) Arrest of Juveniles	19-15
19.12.1 (U) Definition	19-15
19.12.2 (U) Arrest Procedures	19-15
20(U) Other Investigative Resources	20-1
20.1 (U) Overview	20-1
20.1.1 (U//FOUO) Name Trace Requests (CIA and NSA)	20-1
20.1.2 (U//FOUO) Blind Faith Program	20-1
20.1.3 (U//FOUO) Behavioral Analysis – Operational Behavioral Support Program	20-1
20.1.4 (U//FOUO) Sensitive Technical Equipment	20-1
20.2 (U//FOUO) Name Trace Requests (CIA and NSA)	20-1
20.2.1 (U) Authorized Investigative Activity	20-1
20.3 (U//FOUO) Blind Faith Program	20-1
20.3.1 (U) Authorized Investigative Activity	20-2
20.4 (U//FOUO) Operational Behavioral Support Program – CIRG’s Behavioral Analysis Units (BAUs) and/or CD’s Behavioral Analysis Program	20-2
20.4.1 (U) Authorized Investigative Activity	20-2
20.5 (U//FOUO) Sensitive Technical Equipment	20-2
20.5.1 (U) Authorized Investigative Activity	20-2
21(U) Intelligence Collection	21-1
21.1 (U) Incidental Collection	21-1
21.2 (U) FBI National Collection Requirements	21-1
21.3 (U//FOUO) FBI Field Office Collection Requirements	21-2

APPENDICES

Appendix A: (U) The Attorney General's Guidelines for Domestic FBI Operations

Appendix B: (U) Executive Order 12333

Appendix C: (U//FOUO) Use and Targeting of a Federal Prisoner Held in the Custody of the BOP or USMS During an FBI Predicated Investigation; Interview of a Federal Prisoner Held in the Custody of the BOP or USMS During an FBI Assessment or Predicated Investigation

Appendix D: (U) Department of Justice Memorandum on Communications with the White House and Congress, dated May 11, 2009

Appendix E: (U//FOUO) Attorney General Memorandum – Revised Policy on the Use or Disclosure of FISA information, dated January 10, 2008

Appendix F: (U) DOJ Policy on Use of Force

Appendix G: (U) Classified Provisions

Appendix H: (U) Pre-Title III Electronic Surveillance (ELSUR) Search Policy

Appendix I: (U) Accessing Student Records Maintained by an Educational Institution ("Buckley Amendment")

Appendix J: (U) Case File Management and Indexing

Appendix K: (U) Major Cases

Appendix L: (U) On-Line Investigations

Appendix M: (U) The Fair Credit Reporting Act (FCRA)

Appendix N: (U) Tax Return information

Appendix O: (U) Right to Financial Privacy Act (RFPA)

Appendix P: (U) Acronyms

Appendix Q: (U) Definitions

Appendix R: (U) Superseded Documents and NFIPM, MIOG, and MAOP Sections

Appendix S: (U) Lists of Investigative Methods

This Page is Intentionally Blank.

(U) PREAMBLE

August 17, 2011

(U) As the primary investigative agency of the federal government, the FBI has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out criminal investigations and investigations of threats to the national security of the United States. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to counter foreign entities' espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the United States Intelligence Community (USIC). (AGG-Dom, Introduction)

(U) While investigating crime, terrorism, and threats to the national security, and collecting foreign intelligence, the FBI must fully comply with all laws and regulations, including those designed to protect civil liberties and privacy. Through compliance, the FBI will continue to earn the support, confidence and respect of the people of the United States.

(U) To assist the FBI in its mission, the Attorney General signed the *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) on September 29, 2008. The primary purpose of the AGG-Dom and the Domestic Investigations and Operations Guide (DIOG) is to standardize policy so that criminal, national security, and foreign intelligence investigative activities are accomplished in a consistent manner, whenever possible (e.g., same approval, notification, and reporting requirements). In addition to the DIOG, each FBIHQ operational division has a policy implementation guide (PG) that supplements this document. Numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and the operational division policy implementation guides, thus, consolidating the FBI's policy guidance. The FBIHQ Corporate Policy Office (CPO) plays an instrumental role in this endeavor. Specifically, the CPO maintains the most current version of the DIOG on its website. As federal statutes, executive orders, Attorney General guidelines, FBI policies, or other relevant authorities change, CPO will electronically update the DIOG after appropriate coordination and required approvals.

(U) This revised DIOG is a direct result of more than 700 comments received from field and Headquarters employees after release of the initial DIOG in December 2008. Each suggestion was reviewed by a working group comprised of experienced field agents and Chief Division Counsels, as well as representatives from the CPO, the Office of General Counsel (OGC), and the Office of Integrity and Compliance (OIC). Many of these changes and suggestions have been incorporated in the revised DIOG. These changes to the DIOG should better equip you to protect the people of the United States against crime and threats to the national security and to collect foreign intelligence. This is your document, and it requires your input so that we can provide the best service to our nation. If you discover a need for change, please forward your suggestion to FBIHQ CPO.

(U) Thank you for your outstanding service!

Robert S. Mueller, III
Director

1 (U) SCOPE AND PURPOSE

1.1 (U) SCOPE

(U) The Domestic Investigations and Operations Guide (DIOG) applies to all investigative activities and intelligence collection activities conducted by the FBI within the United States, in the United States territories, or outside the territories of all countries. This policy document does not apply to investigative and intelligence collection activities of the FBI in foreign countries; those are governed by:

- A) (U) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations*;
- B) (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (those portions which were not superseded by *The Attorney General Guidelines for Domestic FBI Operations*);
- C) (U) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions*;
- D) (U) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988; and
- E) (U) *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

(U//FOUO) Collectively, these guidelines and procedures are hereinafter referred to as the Extraterritorial Guidelines in the DIOG.

1.2 (U) PURPOSE

(U) The purpose of the DIOG is to standardize policies so that criminal, national security, and foreign intelligence investigative activities are consistently and uniformly accomplished whenever possible (e.g., same approval, opening/closing, notification, and reporting requirements).

(U) This policy document also stresses the importance of oversight and self-regulation to ensure that all investigative and intelligence collection activities are conducted within Constitutional and statutory parameters and that civil liberties and privacy are protected.

(U) In addition to this policy document, each FBI Headquarters (FBIHQ) operational division has a Policy Implementation Guide (PG) or several PGs that supplement the DIOG. These operational division PGs may not contradict, alter, or otherwise modify the standards established in the DIOG. As a result, numerous FBI manuals, electronic communications, letterhead memoranda, and other policy documents are incorporated into the DIOG and operational division PGs, thus, consolidating FBI policy guidance.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

This Page is Intentionally Blank.

2 (U) GENERAL AUTHORITIES AND PRINCIPLES

2.1 (U) AUTHORITY OF THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

(U) The *Attorney General's Guidelines for Domestic FBI Operations* (AGG-Dom) apply to investigative and intelligence collection activities conducted by the FBI within the United States, in the United States territories, or outside the territories of all countries. They do not apply to investigative and intelligence collection activities of the FBI in foreign countries, which are governed by the Extraterritorial Guidelines discussed in DIOG Section 13. (Reference: AGG-Dom, Part I.A.)

(U) The AGG-Dom replaces the following six guidelines:

- A) (U) *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* (May 30, 2002);
- B) (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (October 31, 2003);
- C) (U) *The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence* (November 29, 2006);
- D) (U) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988);
- E) (U) *The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest* (April 5, 1976); and
- F) (U) *The Attorney General's Procedures for Lawful, Warrantless Monitoring of Verbal Communications* (May 30, 2002) [only portion applicable to FBI repealed].

(U) Certain of the existing guidelines that are repealed by the AGG-Dom currently apply in part to extraterritorial operations, including the *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*, and the *Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations*. To ensure that there is no gap in the existence of guidelines for extraterritorial operations, these existing guidelines will remain in effect in their application to extraterritorial operations notwithstanding the general repeal of these existing guidelines by the AGG-Dom.

(U) Also, the classified *Attorney General Guidelines for Extraterritorial FBI Operation and Criminal Investigations* (1993) will continue to apply to FBI criminal investigations, pending the execution of the new guidelines for extraterritorial operations. Finally, for national security and foreign intelligence investigations, FBI investigative activities will continue to be processed as set forth in the classified *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

2.2 (U) GENERAL FBI AUTHORITIES UNDER AGG-Dom

(U) The AGG-Dom recognizes four broad, general FBI authorities. (AGG-Dom, Part I.B.)

2.2.1 (U) CONDUCT INVESTIGATIONS AND COLLECT INTELLIGENCE AND EVIDENCE

(U) The FBI is authorized to collect intelligence and to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in the DIOG (AGG-Dom, Part II).

(U) By regulation, the Attorney General has directed the FBI to investigate violations of the laws of the United States and to collect evidence in investigations in which the United States is or may be a party in interest, except in investigations in which such responsibility is by statute or otherwise specifically assigned to another investigative agency. The FBI's authority to investigate and to collect evidence involving criminal drug laws of the United States is concurrent with such authority of the Drug Enforcement Administration (DEA) (28 C.F.R. § 0.85[a]).

2.2.2 (U) PROVIDE INVESTIGATIVE ASSISTANCE

(U) The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal agencies, and foreign agencies as provided in Section 12 of the DIOG (AGG-Dom, Part III).

2.2.3 (U) CONDUCT INTELLIGENCE ANALYSIS AND PLANNING

(U) The FBI is authorized to conduct intelligence analysis and planning as provided in Section 15 of the DIOG (AGG-Dom, Part IV).

2.2.4 (U) RETAIN AND SHARE INFORMATION

(U) The FBI is authorized to retain and to share information obtained pursuant to the AGG-Dom, as provided in Sections 12 and 14 of the DIOG (AGG-Dom, Part VI).

2.3 (U) FBI AS AN INTELLIGENCE AGENCY

(U) The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See Executive Order 12333; 28 U.S.C. § 532 note (incorporating P.L. 108-458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107).

(U) Part IV of the AGG-Dom authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part includes: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests; (ii) research and analysis to produce reports and assessments (see note below) concerning matters relevant to investigative activities or other authorized FBI activities;

and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

(U) *Note:* In the DIOG, the word “assessment” has two distinct meanings. The AGG-Dom authorizes as an investigative activity an “Assessment,” which requires an authorized purpose and objective (s) as discussed in the DIOG Section 5. The United States Intelligence Community (USIC), however, also uses the word “assessment” to describe written intelligence products as discussed in the DIOG Section 15.6.1.2.

2.4 (U) FBI LEAD INVESTIGATIVE AUTHORITIES

2.4.1 (U) INTRODUCTION

(U//FOUO) The FBI’s primary investigative authority is derived from the authority of the Attorney General as provided in 28 U.S.C. §§ 509, 510, 533 and 534. Within this authority, the Attorney General may appoint officials to detect crimes against the United States and to conduct such other investigations regarding official matters under the control of the Department of Justice (DOJ) and the Department of State (DOS) as may be directed by the Attorney General (28 U.S.C. § 533). The Attorney General has delegated a number of his statutory authorities and granted other authorities to the Director of the FBI (28 C.F.R. § 0.85[a]). Some of these authorities apply both inside and outside the United States.

2.4.2 (U) TERRORISM AND COUNTERTERRORISM INVESTIGATIONS

(U) The Attorney General has directed the FBI to exercise Lead Agency responsibility in investigating all crimes for which DOJ has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States. Within the United States, this includes the collection, coordination, analysis, management and dissemination of intelligence and criminal information, as appropriate. If another federal agency identifies an individual who is engaged in terrorist activities or acts in preparation of terrorist activities, the other agency is required to promptly notify the FBI. Terrorism, in this context, includes the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, to further political or social objectives (28 C.F.R. § 0.85[I]). For a current list of legal authorities relating to the FBI’s investigative jurisdiction in terrorism investigations, see the OGC Law Library website at <http://home.fbinet.fbi/DO/OGC/Pages/MainLawLibrary.aspx>.

(U//FOUO) DOJ guidance designates the FBI as Lead Agency for investigating explosives matters which, under the following protocol, demonstrate a possible nexus to international or domestic terrorism:

- A) (U//FOUO) The following factors are strong indicia of a nexus to terrorism and lead-agency jurisdiction is assigned based on these factors alone:*
- 1) (U//FOUO) an attack on a government building, mass transit, a power plant; or*
 - 2) (U//FOUO) the use of a chemical, biological, radiological, or nuclear agents.*

- B) (U//FOUO) Requires each agency to notify the other immediately when responding to an explosives incident and to share all relevant information that may serve to rule in or out a connection to terrorism; and
- C) (U//FOUO) Creates a process for the FBI/Joint Terrorism Task Force (JTTF) to identify an explosives incident as connected to terrorism when there is reliable evidence supporting that claim and establishes a process for shifting lead-agency jurisdiction to the JTTF until the issue is resolved. (See DOJ Memorandum, dated August 3, 2010, on "Protocol for Assigning Lead Agency Jurisdiction in Explosives Investigations.")

2.4.2.1 (U) "FEDERAL CRIMES OF TERRORISM"

(U) Pursuant to the delegation in 28 C.F.R. § 0.85(I), the FBI exercises the Attorney General's lead investigative responsibility under 18 U.S.C. § 2332b(f) for all "federal crimes of terrorism" as identified in that statute. Many of these statutes grant the FBI extraterritorial investigative responsibility (See the cited statute for the full particulars concerning elements of the offense, jurisdiction, etc.). Under 18 U.S.C. § 2332b(g)(5), the term "federal crime of terrorism" means an offense that is: (i) calculated to influence or affect the conduct of government by intimidation or coercion or to retaliate against government conduct; and (ii) violates a federal statute relating to:

- A) (U) Destruction of aircraft or aircraft facilities (18 U.S.C. § 32);
- B) (U) Violence at international airports (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 37);
- C) (U) Arson within "special maritime and territorial jurisdiction (SMTJ) of the United States" (SMTJ is defined in 18 U.S.C. § 7) (18 U.S.C. § 81);
- D) (U) Prohibitions with respect to biological weapons (extraterritorial federal jurisdiction if offense committed by or against a United States national) (18 U.S.C. § 175);
- E) (U) Possession of biological agents or toxins by restricted persons (18 U.S.C. § 175b);
- F) (U) Variola virus (includes smallpox and other derivatives of the variola major virus) (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 175c);
- G) (U) Prohibited activities regarding chemical weapons (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 229) (E.O. 13128 directs any possible violation of this statute be referred to the FBI);
- H) (U) Congressional, Cabinet, and Supreme Court assassination, kidnapping and assault (18 U.S.C. § 351[a]-[d]) (18 U.S.C. § 351[g] directs that the FBI shall investigate violations of this statute);
- I) (U) Prohibited transactions involving nuclear materials (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 831);
- J) (U) Participation in nuclear and weapons of mass destruction threats to the United States (extraterritorial federal jurisdiction) (18 U.S.C. § 832);
- K) (U) Importation, exportation, shipping, transport, transfer, receipt, or possession of plastic explosives that do not contain a detection agent (18 U.S.C. § 842[m] and [n]);
- L) (U) Arson or bombing of government property risking or causing death (18 U.S.C. § 844[f][2] or [3]) (18 U.S.C. § 846[a] grants FBI and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) concurrent authority to investigate violations of this statute). See Section

2.4.2.1.L above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;

- M) (U) Arson or bombing of property used in or affecting interstate or foreign commerce (18 U.S.C. § 844[i]) (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute);
- N) (U) Killing or attempted killing during an attack on a federal facility with a dangerous weapon (18 U.S.C. § 930[c]);
- O) (U) Conspiracy within United States jurisdiction to murder, kidnap, or maim persons at any place outside the United States (18 U.S.C. § 956[a][1]);
- P) (U) Using a computer for unauthorized access, transmission, or retention of protected information (18 U.S.C. § 1030[a][1]) (18 U.S.C. § 1030[d][2] grants the FBI “primary authority” to investigate Section 1030[a][1] offenses involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data as defined in the Atomic Energy Act, except for offenses affecting United States Secret Service (USSS) duties under 18 U.S.C. § 3056[a]);
- Q) (U) Knowingly transmitting a program, information, code, or command and thereby intentionally causing damage, without authorization, to a protected computer (18 U.S.C. § 1030[a][5][A][i]);
- R) (U) Killing or attempted killing of officers or employees of the United States, including any member of the uniformed services (18 U.S.C. § 1114);
- S) (U) Murder or manslaughter of foreign officials, official guests, or internationally protected persons (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 1116) (Attorney General may request military assistance in the course of enforcement of this section);
- T) (U) Hostage taking (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 1203);
- U) (U) Willfully injuring or committing any depredation against government property or contracts (18 U.S.C. § 1361);
- V) (U) Destruction of communication lines, stations, or systems (18 U.S.C. § 1362);
- W) (U) Destruction or injury to buildings or property within special maritime and territorial jurisdiction of the United States (18 U.S.C. § 1363);
- X) (U) Destruction of \$100,000 or more of an “energy facility” property as defined in the statute (18 U.S.C. § 1366);
- Y) (U) Presidential and Presidential staff assassination, kidnapping, and assault (18 U.S.C. § 1751[a], [b], [c], or [d]) (extraterritorial jurisdiction) (Per 18 U.S.C. § 1751[i], 1751 violations must be investigated by the FBI; FBI may request assistance from any federal [including military], state, or local agency notwithstanding any statute, rule, or regulation to the contrary);
- Z) (U) Terrorist attacks and other violence against railroad carriers and against mass transportation systems on land, on water, or through the air (includes a school bus, charter, or sightseeing transportation; or any means of transport on land, water, or through the air) (18 U.S.C. § 1992);
- AA) (U) Destruction of national defense materials, premises, or utilities (18 U.S.C. § 2155);

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- BB) (U) *Production of defective national defense materials, premises, or utilities (18 U.S.C. § 2156);*
- CC) (U) *Violence against maritime navigation (18 U.S.C. § 2280);*
- DD) (U) *Violence against maritime fixed platforms (located on the continental shelf of the United States or located internationally in certain situations) (18 U.S.C. § 2281);*
- EE) (U) *Certain homicides and other violence against United States nationals occurring outside of the United States (18 U.S.C. § 2332);*
- FF) (U) *Use of weapons of mass destruction (WMD) (against a national of the United States while outside the United States; against certain persons or property within the United States; or by a national of the United States outside the United States) (18 U.S.C. § 2332a) (WMD defined in 18 U.S.C. § 2332a[c][2]);*
- GG) (U) *Acts of terrorism transcending national boundaries (includes murder, kidnapping, and other prohibited acts occurring inside and outside the United States under specified circumstances – including that the victim is a member of a uniform service; includes offenses committed in the United States territorial sea and airspace above and seabed below; includes offenses committed in special maritime and territorial jurisdiction of the United States as defined in 18 U.S.C. § 7) (18 U.S.C. § 2332b);*
- HH) (U) *Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities (applies to offenses occurring inside or outside the United States in certain situations; does not apply to activities of armed forces during an armed conflict) (18 U.S.C. § 2332f);*
- II) (U) *Missile systems designed to destroy aircraft (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 2332g);*
- JJ) (U) *Radiological dispersal devices (applies to offenses occurring outside the United States in certain situations) (18 U.S.C. § 2332h);*
- KK) (U) *Harboring or concealing terrorists (18 U.S.C. § 2339);*
- LL) (U) *Providing material support or resources to terrorists (18 U.S.C. § 2339A);*
- MM) (U) *Providing material support or resources to designated foreign terrorist organizations (extraterritorial federal jurisdiction) (18 U.S.C. § 2339B) ("The Attorney General shall conduct any investigation of a possible violation of this section, or of any license, order, or regulation issued pursuant to this section." 18 U.S.C. § 2339B[e][1]);*
- NN) (U) *Prohibitions against the financing of terrorism (applies to offenses occurring outside the United States in certain situations including on board a vessel flying the flag of the United States or an aircraft registered under the laws of the United States) (18 U.S.C. § 2339C) (Memorandum of Agreement between the Attorney General and the Secretary of Homeland Security, dated May 13, 2005; FBI leads all terrorist financing investigations and operations);*
- OO) (U) *Relating to military-type training from a foreign terrorist organization (extraterritorial jurisdiction) (18 U.S.C. § 2339D);*
- PP) (U) *Torture applies only to torture committed outside the United States in certain situations; torture is defined in 18 U.S.C. § 2340 (18 U.S.C. § 2340A);*
- QQ) (U) *Prohibitions governing atomic weapons (applies to offenses occurring outside the United States in certain situations) (42 U.S.C. § 2122) (FBI shall investigate alleged or suspected violations per 42 U.S.C. § 2271[b]);*

- RR) (U) Sabotage of nuclear facilities or fuel (42 U.S.C. § 2284) (FBI shall investigate alleged or suspected violations per 42 U.S.C. § 2271[b]);
- SS) (U) Aircraft piracy (applies to offenses occurring outside the United States in certain situations) (49 U.S.C. § 46502) (FBI shall investigate per 28 U.S.C. § 538);
- TT) (U) Assault on a flight crew with a dangerous weapon (applies to offenses occurring in the "special aircraft jurisdiction of the United States" as defined in 49 U.S.C. § 46501[2]); (second sentence of 49 U.S.C. § 46504) (FBI shall investigate per 28 U.S.C. § 538);
- UU) (U) Placement of an explosive or incendiary device on an aircraft (49 U.S.C. § 46505[b][3]) (FBI shall investigate per 28 U.S.C. § 538);
- VV) (U) Endangerment of human life on aircraft by means of weapons (49 U.S.C. § 46505[c]) (FBI shall investigate per 28 U.S.C. § 538);
- WW) (U) Application of certain criminal laws to acts on aircraft (if homicide or attempted homicide is involved) (applies to offenses occurring in the "special aircraft jurisdiction of the United States" as defined in 18 U.S.C. § 46501[2]); (49 U.S.C. § 46506) (FBI shall investigate per 28 U.S.C. § 538);
- XX) (U) Damage or destruction of interstate gas or hazardous liquid pipeline facility (49 U.S.C. § 60123[b]); and
- YY) (U) Section 1010A of the Controlled Substances Import and Export Act (relating to narco-terrorism).

2.4.2.2 (U) ADDITIONAL OFFENSES NOT DEFINED AS "FEDERAL CRIMES OF TERRORISM"

(U) Title 18 U.S.C. § 2332b(f) expressly grants the Attorney General primary investigative authority for additional offenses not defined as "Federal Crimes of Terrorism." These offenses are:

- A) (U) Congressional, Cabinet, and Supreme Court assaults (18 U.S.C. § 351[e]) (18 U.S.C. § 351[g]) directs that the FBI investigate violations of this statute;
- B) (U) Using mail, telephone, telegraph, or other instrument of interstate or foreign commerce to threaten to kill, injure, or intimidate any individual, or unlawfully to damage or destroy any building, vehicle, or other real or personal property by means of fire or explosive (18 U.S.C. § 844[e]); (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute);
- C) (U) Damages or destroys by means of fire or explosive any building, vehicle, or other personal or real property, possessed, owned, or leased to the United States or any agency thereof, or any institution receiving federal financial assistance (18 U.S.C. § 844[f][1]) (18 U.S.C. § 846[a] grants FBI and ATF concurrent authority to investigate violations of this statute). See Section 2.4.2.1.L above regarding DOJ Memorandum dated 08/03/2010 on ATF/FBI Lead Agency Jurisdiction;
- D) (U) Conspiracy within United States jurisdiction to damage or destroy property in a foreign country and belonging to a foreign country, or to any railroad, canal, bridge, airport, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated (18 U.S.C. § 956[b]);
- E) (U) Destruction of \$5,000 or more of an "energy facility" property as defined in 18 U.S.C. § 1366(c) (18 U.S.C. § 1366[b]); and

F) (U) Willful trespass upon, injury to, destruction of, or interference with fortifications, harbor defenses, or defensive sea areas (18 U.S.C. § 2152).

(U) Nothing in this section of the DIOG may be construed to interfere with the USSS under 18 U.S.C. § 3056.

2.4.2.3 (U//FOUO) NSPD-46/HSPD-15, "U.S. POLICY AND STRATEGY IN THE WAR ON TERROR"

(U//FOUO) Annex II (Consolidation and Updating of Outdated Presidential Counterterrorism Documents), dated January 10, 2007, to the classified National Security Presidential Directive (NSPD) 46/Homeland Security Presidential Directive (HSPD) 15, dated March 6, 2006, establishes FBI lead responsibilities, as well as those of other federal entities, in the "War on Terror." Annex II directs departments or agencies with lead or primary responsibility under the Annex "to coordinate – through the appropriate mechanism – their discharge of such responsibility with other relevant departments and agencies, except where indicated otherwise in the Annex."

(U//FOUO) Areas addressed in Annex II include domestic incident management, continuity of operations/continuity of government, air piracy and hijacking, National Special Security Events (NSSE), maritime domain, WMD interdiction, critical infrastructure protection, and disrupting terrorists at home and abroad. Both NSPD-46/HSPD-15 and Annex II thereto are classified.

2.4.3 (U) COUNTERINTELLIGENCE AND ESPIONAGE INVESTIGATIONS

(U//FOUO) A representative list of federal statutes applicable to counterintelligence and espionage investigations appears below. For additional information, refer to the classified Counterintelligence Division (CD) Policy Implementation Guide (PG) and the current list of espionage and counterintelligence authorities.

2.4.3.1 (U) ESPIONAGE INVESTIGATIONS OF PERSONS IN UNITED STATES DIPLOMATIC MISSIONS ABROAD

(U) Section 603 of the Intelligence Authorization Act of 1990 (P.L. 101-193) states that, subject to the authority of the Attorney General, "the FBI shall supervise the conduct of all investigations of violations of the espionage laws of the United States by persons employed by or assigned to United States diplomatic missions abroad. All departments and agencies shall provide appropriate assistance to the FBI in the conduct of such investigations." Consult the Attorney General's extraterritorial guidelines and other applicable policy or agreements.

2.4.3.2 (U) INVESTIGATIONS OF UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION TO A FOREIGN POWER OR AGENT OF A FOREIGN POWER

(U) The National Security Act of 1947, as amended, establishes procedures for the coordination of counterintelligence activities (50 U.S.C. § 402a). Part of that statute requires that, absent extraordinary circumstances as approved by the President in writing on a case-by-case basis, the head of each executive branch department or agency must ensure that the FBI is "advised immediately of any information, regardless of its origin, which indicates that

classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.”

2.4.4 (U) CRIMINAL INVESTIGATIONS

(U//FOUO) In addition to the statutes listed above and below, refer to the appropriate program/sub-program Criminal Investigative Division (CID) PG for additional criminal jurisdiction information.

2.4.4.1.1 (U) INVESTIGATIONS OF AIRCRAFT PRIVACY AND RELATED VIOLATIONS

(U) The FBI shall investigate any violation of 49 U.S.C. § 46314 (Entering aircraft or airport areas in violation of security requirements) or chapter 465 (Special aircraft jurisdiction of the United States) of Title 49, United States Code; (28 U.S.C. § 538)

2.4.4.1.2 (U) VIOLENT CRIMES AGAINST FOREIGN TRAVELERS

(U) The Attorney General and Director of the FBI shall assist state and local authorities in investigating and prosecuting a felony crime of violence in violation of the law of any State in which the victim appears to have been selected because he or she is a traveler from a foreign nation; (28 U.S.C. § 540A[b])

2.4.4.1.3 (U) FELONIOUS KILLINGS OF STATE AND LOCAL LAW ENFORCEMENT OFFICERS

(U) The FBI shall investigate any violation of 28 U.S.C. § 540; and

2.4.4.1.4 (U) INVESTIGATIONS OF SERIAL KILLINGS

(U) The FBI shall investigate any violation of 28 U.S.C. § 540B.

2.4.5 (U) AUTHORITY OF AN FBI SPECIAL AGENT

(U) An FBI Special Agent has the authority to:

- A) (U) Investigate violations of the laws, including the criminal drug laws, of the United States (21 U.S.C. § 871; 28 U.S.C. §§ 533, 534 and 535; 28 C.F.R. § 0.85);
- B) (U) Collect evidence in investigations in which the United States is or may be a party in interest (28 C.F.R. § 0.85 [a]) as redelegated through exercise of the authority contained in 28 C.F.R. § 0.138 to direct personnel in the FBI;
- C) (U) Make arrests (18 U.S.C. §§ 3052 and 3062);
- D) (U) Serve and execute arrest warrants and seize property under warrant; issue and/or serve administrative subpoenas; serve subpoenas issued by other proper authority; and make civil investigative demands (18 U.S.C. §§ 3052, 3107; 21 U.S.C. § 876; 15 U.S.C. § 1312);
- E) (U) Carry firearms (18 U.S.C. § 3052);
- F) (U) Administer oaths to witnesses attending to testify or depose in the course of investigations of frauds on or attempts to defraud the United States or irregularities or misconduct of employees or agents of the United States (5 U.S.C. § 303);

G) (U) Seize property subject to seizure under the criminal and civil forfeiture laws of the United States (e.g., 18 U.S.C. §§ 981 and 982); and

H) (U) Perform other duties imposed by law.

(U) Note: For policy regarding Agent's authority to intervene in non-federal crimes or make non-federal arrests, see Section 19.3.3.

2.5 (U) STATUS AS INTERNAL GUIDANCE

(U) The AGG-Dom, this DIOG, and the various operational division PGs are set forth solely for the purpose of internal DOJ and FBI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the DOJ and the FBI. (AGG-Dom, Part I.D.2.)

2.6 (U) DEPARTURE FROM THE AGG-DOM (AGG-DOM I.D.3)

2.6.1 (U) DEFINITION

(U//FOUO) A "departure" from the AGG-Dom is a deliberate deviation from a known requirement of the AGG-Dom. The word "deliberate" means the employee was aware of the AGG-Dom requirement and affirmatively chose to depart from it for operational reasons before the activity took place. Departures from the AGG-Dom may only be made in accordance with the guidance provided in this section.

2.6.2 (U) DEPARTURE FROM THE AGG-DOM IN ADVANCE

(U//FOUO) A departure from the AGG-Dom must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director (EAD) designated by the Director. The Director of the FBI has designated the EAD National Security Branch (NSB) and the EAD Criminal Cyber Response and Services Branch (CCRSB) to grant departures from the AGG-Dom. Notice of the departure must be provided by Electronic Communication (EC) to the General Counsel (GC) using file number 333-HQ-C1629406. The Office of the General Counsel (OGC) must provide timely written notice of departures from the AGG-Dom to either the DOJ Criminal Division or National Security Division (NSD), whichever is appropriate, or to both, and the Criminal Division or NSD must notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (AGG-Dom, Part I.D.3.)

2.6.3 (U) EMERGENCY DEPARTURES FROM THE AGG-DOM

(U//FOUO) If a departure from the AGG-Dom is necessary without prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, an FBI employee may, at his/her discretion, depart from the requirements of the AGG-Dom when the designated approving authority for the investigative activity cannot be contacted through reasonable means. The Director, the Deputy Director, or a designated EAD, and the GC must be notified by EC of the departure as soon thereafter as practicable, but not more than 5 business days after the departure using file number 333-HQ-C1629406. The OGC must provide

timely written notice of departures from the AGG-Dom to either the DOJ Criminal Division or NSD, whichever is appropriate, or to both of them, and the Criminal Division or NSD must notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States. (AGG-Dom, Part I.D.3.)

2.6.4 (U) RECORDS OF DEPARTURES FROM THE AGG-DOM

(U//FOUO) The OGC is responsible for maintaining records of all requests and approvals or denials of departures from the AGG-Dom. Records will be maintained in file number 333-HQ-C1629406.

2.7 (U) DEPARTURES FROM THE DIOG

2.7.1 (U) DEFINITION

(U//FOUO) A “departure” from the DIOG is a deliberate deviation from a known requirement of the DIOG. The word “deliberate” means the employee was aware of the DIOG requirement and affirmatively chose to depart from it for operational reasons before the activity took place. Departures from the DIOG may only be made in accordance with the guidance provided in this section.

2.7.2 (U) DEPARTURE FROM THE DIOG

(U//FOUO) A request for a departure from the DIOG must be submitted with an EC using file number 333-HQ-C1629406 and approved by the appropriate operational program Assistant Director (AD) with notice to the GC. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

(U//FOUO) OGC will review all departures from the DIOG. If OGC determines the departure from the DIOG also involves a departure from the AGG-Dom, OGC must provide timely written notice to DOJ in accordance with the provisions of Section I.D.3 of the AGG-Dom.

2.7.3 (U) EMERGENCY DEPARTURES FROM THE DIOG

(U//FOUO) FBI employees may conduct or engage in investigative activity that deviates from the requirements of the DIOG, including utilizing investigative methods, without prior approval, when the designated approving authority for the investigative activity (if any) cannot be contacted through reasonable means and in the judgment of the employee one of the following factors is present:

A) (U//FOUO) an immediate or grave threat to the safety of persons or property exists, or

B) (U//FOUO) an immediate or grave threat to the national security exists, or

C) (U//FOUO) a substantial likelihood exists that a delay will result in the loss of a significant investigative opportunity.¹

(U//FOUO) The appropriate operational program AD and the GC must be notified of the emergency departure by EC using file number 333-HQ-C1629406 as soon as practicable, but no later than 5 business days after engaging in the activity or utilizing the investigative method. This documentation must also be filed in the applicable investigative file in which the activity or method was taken. OGC will review all departures from the DIOG. If OGC determines the departure from the DIOG also involves a departure from the AGG-Dom, OGC must provide timely written notice to DOJ in accordance with the provisions of Section I.D.3 of the AGG-Dom. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

2.7.4 (U) RECORDS OF DEPARTURES FROM THE DIOG

(U//FOUO) The OGC is responsible for maintaining records of all requests and approvals or denials of departures from the DIOG. Records will be maintained in file number 333-HQ-C1629406.

2.8 (U) DISCOVERY OF NON-COMPLIANCE WITH DIOG REQUIREMENTS AFTER-THE-FACT

2.8.1 (U) SUBSTANTIAL NON-COMPLIANCE WITH THE DIOG

2.8.1.1 (U) SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) “Substantial non-compliance” means non-compliance that is of significance to the matter and is more than a minor deviation from a DIOG requirement.² Non-compliance that relates solely to administrative or peripheral requirements is not substantial. Substantial non-compliance specifically includes the following:

- A) (U//FOUO) the unauthorized use of an investigative method;*
- B) (U//FOUO) the failure to obtain required supervisory approval;³ and*
- C) (U//FOUO) non-compliance that has a potential adverse effect upon a member of the public’s individual rights or liberties.*

(U//FOUO) **Example A:** During an Assessment, ASAC approval was not obtained before using the Mobile Surveillance Team (MST) and the Bureau airplane to conduct surveillance. Because the approval was not obtained in advance nor was it done pursuant to an emergency

¹ (U//FOUO) This is not a permissible factor for departing from the AGG-Dom. Thus, this factor may only provide a basis for a departure from the DIOG that does not require a departure from the AGG-Dom.

² (U//FOUO) Departures from the AGG-Dom and the DIOG do not fall within the definition of “non-compliance” as used in this section. Departures are to be handled as described Sections 2.6 and 2.7 and should not be reported as “non-compliance” matters.

³ (U//FOUO) If supervisory approval was obtained pursuant to Section 2.7.3 (Emergency Departure from the DIOG), the failure to document this approval within 5 business days is a reportable “substantial non-compliance” matter.

situation as described in 2.7.3, this would be “substantial” non-compliance with DIOG sections 18.5.8.3.3 and 18.5.8.3.4 and must be reported to OIC as set forth in 2.8.2 below.

(U//FOUO) **Example B:** A new SSA arrives in a squad and discovers that his predecessor did not conduct file reviews in several of the squad’s Predicated Investigations for several months. This is “substantial non-compliance” and must be reported.

2.8.1.2 (U) OTHER NON-COMPLIANCE

(U//FOUO) Non-compliance with the DIOG that is not “substantial” may be reported, but it is not mandatory to do so. If there is uncertainty regarding whether a particular matter is substantial or not, the matter should be reported. Nevertheless, whenever non-compliance is discovered (whether reported or not), appropriate remedial action must be taken by the relevant employee(s) to correct the non-compliance, including implementing any preventative measures that would help eliminate possible future non-compliance.

(U//FOUO) **Example:** An SSA discovers that she conducted a file review 20 days late. This relates to an administrative requirement and, without more, is not “substantial” noncompliance; this does not have to be reported to OIC. The SSA should, however, take appropriate preventative measures to avoid recurrence.

2.8.2 (U) DOCUMENTATION OF SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) Substantial non-compliance with the DIOG must be reported by EC or subsequent form. The EC must include the following information:

- A) (U//FOUO) *The relevant DIOG provision(s) involved;*
- B) (U//FOUO) *Description of the facts and circumstances (including dates) of the substantial non-compliance;*
- C) (U//FOUO) *The date the substantial non-compliance was discovered;*
- D) (U//FOUO) *Circumstances leading to the discovery of the substantial non-compliance;*
- E) (U//FOUO) *If the substantial non-compliance was the result of the failure to obtain appropriate supervisory approval (e.g., failure to comply with the requirements of section 2.7.4) in the context of an emergency departure from the DIOG, a statement as to whether that official, or the current official in the appropriate supervisory position, would have approved the action if a timely request had been made based on the facts and circumstances then known;*
- F) (U//FOUO) *Known adverse consequences, if any, attributable to the substantial non-compliance; and*
- G) (U//FOUO) *Corrective or remedial action(s) taken or planned to be taken to mitigate the substantial non-compliance, as well as to help prevent such occurrences in the future.*

(U//FOUO) **Example:** An ASAC discovers that a Preliminary Investigation (PI) was extended without obtaining the proper approvals. The failure to obtain appropriate supervisory approval to extend the Preliminary Investigation must be reported, and the report must address all of the seven areas in A-G listed above.

2.8.3 (U) REPORTING AUTHORITIES

(U//FOUO) If the substantial non-compliance occurred in a field office, the EC must be addressed to the ADIC/SAC. If the substantial non-compliance occurred at FBI Headquarters (FBIHQ), the EC must be addressed to the employee's Assistant Director. A copy of the EC must be provided to the Office of Integrity and Compliance (OIC) and to the Office of the General Counsel (OGC) using file number 319O-HQ-A1561245-OIC. A copy of the EC should also be sent to the investigative file in which the incident occurred. In addition, if the ADIC/SAC or AD assesses that the non-compliance appears to reflect intentional or willful misconduct, it must be reported separately by EC to the Internal Investigations Section of the Inspection Division.

2.8.4 (U) ROLE OF OIC AND OGC

(U//FOUO) OGC will review all reports of substantial non-compliance to determine whether any further action is required in the particular matter. OIC will analyze substantial non-compliance reports to determine whether any trends exist in the data and will develop strategies to reduce the occurrences of substantial non-compliance. Based upon OIC's analysis of these reports, if OIC discovers a systemic problem of non-compliance with the AGG-Dom or DIOG involving intelligence activities, either division or FBI wide, OIC must notify OGC/NSLB of this systemic problem.

(U//FOUO) **Example A:** An IA discovers that a mail cover was used in an Assessment. Because mail covers are not permitted to be used in Assessments, this must be reported as a "substantial" non-compliance with the DIOG.

(U//FOUO) **Example B:** A supervisor determines that a Type 1 & 2 Assessment was opened based solely on the exercise of First Amendment rights. While no supervisory approval was required to open the Type 1 & 2 Assessment, this must be reported as "substantial" non-compliance because opening an Assessment based solely on First Amendment activity affects an individual's rights and liberties.

2.8.5 (U) POTENTIAL IOB MATTERS INVOLVING THE REPORTS OF SUBSTANTIAL NON-COMPLIANCE

(U//FOUO) If the substantial non-compliance is also a potential IOB matter, the matter must be reported in accordance with the requirements and procedures for reporting potential IOB matters to OGC/NSLB. See Corporate Policy Directive 0188D: Guidance on Intelligence Oversight Board Matters (See 0188D); the Policy Implementation Guide 0188PG; and see DIOG Section 4. No additional reporting of the incident needs to be made to OIC under this section.

2.8.6 (U) REPORTING NON-COMPLIANCE WITH POLICY IMPLEMENTATION GUIDES

(U//FOUO) Substantial non-compliance with DIOG-related Policy/Program Guides must be reported by EC or subsequent form to the SAC/ADIC, with a copy to the pertinent Headquarters Program Manager, and to the OIC and OGC using file number 319O-HQ-A1561245-OIC.

2.8.7 (U) REPORTING NON-COMPLIANCE WITH OTHER FBI POLICIES AND PROCEDURES (OUTSIDE THE DIOG)

(U//FOUO) Nothing in this section is intended to alter, limit, or restrict existing policies that require non-compliance to be reported in areas not covered by the DIOG. Employees remain responsible to report those other matters. Additional information can be found on [the Office of Integrity and Compliance's webpage](#).

2.9 (U) OTHER FBI ACTIVITIES NOT LIMITED BY AGG-DOM

(U) The AGG-Dom apply to FBI domestic investigative activities and do not limit other authorized activities of the FBI. The authority for such other activities may be derived from the authority of the Attorney General as provided in federal statutes, guidelines, or Executive Orders. The scope and approval of these other authorized activities are addressed in the policies that govern the activity and these policies must be relied on when engaging in such activities. Examples of authorized FBI activities not governed by the AGG-Dom include, but are not limited to, the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs (e.g., background investigations), FBI physical building security issues, Office of Professional Responsibility/personnel issues, certain administrative claims/civil actions, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory. (AGG-Dom, Part I.D.4.)

(U) FBI employees may incidentally obtain information relating to matters outside of the FBI's primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. Neither the AGG-Dom nor the DIOG bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other jurisdictions. (See Section 14; AGG-Dom, Part II and Part VI.B)

2.10 (U) USE OF CLASSIFIED INVESTIGATIVE TECHNOLOGIES

(U) Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases (AGG-Dom, Part V.B.2), Operational Technology Division (OTD) Domestic Technical Assistance (DTA) Policy Implementation Guide (PG), and any other FBI policies concerning such technology use.

2.11 (U) APPLICATION OF AGG-DOM AND DIOG

(U//FOUO) The AGG-Dom and DIOG apply to all FBI domestic investigations and operations conducted by an "FBI employee" or an FBI confidential human source (CHS), when operating

pursuant to the tasking or instructions of an FBI employee. The term “FBI employee” includes, but is not limited to, an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. Both an “FBI employee” and a CHS, when operating pursuant to the tasking or instructions of an FBI employee, are bound by the AGG-Dom and DIOG. In the DIOG, “FBI employee” includes all personnel descriptions, if not otherwise prohibited by law or policy. For example, if the DIOG states that the “FBI employee” is responsible for a particular investigative activity, the supervisor has the flexibility to assign that responsibility to any person bound by the AGG-Dom and DIOG (e.g., agent, intelligence analyst, task force officer), if not otherwise prohibited by law or policy.

(U//FOUO) TFOs, TFMs, TFPs, detailees, and FBI contractors are defined as “FBI employees” for purposes of application of the AGG-Dom and DIOG. However, for overt representational purposes, TFOs, TFMs, TFPs, detailees and FBI contractors should identify themselves as employees of their parent agency and, if appropriate and necessary, affiliated with a particular FBI investigative entity, such as the JTTF, etc. A CHS is likewise bound by the AGG-Dom, DIOG, AGG-CHS, and other applicable CHS policies when operating pursuant to the tasking or instructions of an FBI employee; however, the FBI CHS is not an employee of the FBI.

(U//FOUO) TFOs, TFMs, TFPs, detailees, and FBI contractors are defined as “FBI employees” only for purposes of the AGG-Dom and DIOG. This inclusive definition does not define federal employment for purposes of the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b), 2401, and 2671 et seq.; the Federal Employees Compensation Act, 5 U.S.C. § 8101 et seq.; the Intergovernmental Personnel Act, 5 U.S.C. § 3374 et seq., or any other law.

(U//FOUO) FBIHQ division PGs may not contradict, alter or otherwise modify the standards established in the DIOG.

3 (U) CORE VALUES, ROLES, AND RESPONSIBILITIES

3.1 (U) THE FBI'S CORE VALUES

(U) The FBI's core values guide and further our mission and help us achieve our many goals. The values do not exhaust the many goals we wish to achieve, but they capsuleate the goals as well as can be done in a few words. The FBI's core values must be fully understood, practiced, shared, vigorously defended, and preserved. The values are:

- A) (U) Rigorous obedience to the Constitution of the United States
- B) (U) Respect for the dignity of all those we protect
- C) (U) Compassion
- D) (U) Fairness
- E) (U) Uncompromising personal integrity and institutional integrity
- F) (U) Accountability by accepting responsibility for our actions and decisions and their consequences
- G) (U) Leadership, by example, both personal and professional

(U) By observing these core values, we achieve a high level of excellence in performing the FBI's national security and criminal investigative functions as well as the trust of the American people. Our individual and institutional rigorous obedience to constitutional principles and guarantees is more important than the outcome of any single interview, search for evidence, or investigation. Respect for the dignity of all reminds us to wield law enforcement powers with restraint and to avoid placing our self interest above that of those we serve. Fairness and compassion ensure that we treat everyone with the highest regard for constitutional, civil, and human rights. Personal and institutional integrity reinforce each other and are owed to our Nation in exchange for the sacred trust and great authority conferred upon us.

(U) We who enforce the law must not merely obey it. We have an obligation to set a moral example that those whom we protect can follow. Because the FBI's success in accomplishing its mission is directly related to the support and cooperation of those we protect, these core values are the fiber that holds together the vitality of our institution.

3.1.1 (U) COMPLIANCE

(U) All FBI personnel must fully comply with all laws, rules, and regulations governing FBI investigations, operations, programs and activities, including those set forth in the AGG-Dom. We cannot, do not, and will not countenance disregard for the law for the sake of expediency in anything we do. The FBI expects its personnel to ascertain the laws and regulations that govern the activities in which they engage and to acquire sufficient knowledge of those laws, rules, and regulations to understand their requirements, and to conform their professional and personal conduct accordingly. Under no circumstances will expediency justify disregard for the law. FBI policy must be consistent with Constitutional, legal, and regulatory requirements. Additionally,

the FBI must provide sufficient training to affected personnel and ensure that appropriate oversight monitoring mechanisms are in place.

(U//FOUO) In general, the FBI requires employees to report known or suspected failures to adhere to the law, rules or regulations by themselves or other employees, to any supervisor in the employees' chain of command; any Division Compliance Officer; any Office of the General Counsel (OGC) Attorney; any Inspection Division personnel; any FBI Office of Integrity and Compliance (OIC) staff; or any person designated to receive disclosures pursuant to the FBI Whistleblower Protection Regulation (28 Code of Federal Regulations § 27.1), including the Department of Justice (DOJ) Inspector General. For specific requirements and procedures for reporting "departures" and "non-compliance" with the AGG-Dom on the DIOG, see DIOG Section 2.

3.2 (U) INVESTIGATIVE AUTHORITY, ROLES AND RESPONSIBILITY OF THE DIRECTOR'S OFFICE

3.2.1 (U) DIRECTOR'S AUTHORITY, ROLES AND RESPONSIBILITY

(U//FOUO) The Director's authority is derived from a number of statutory and regulatory sources. For example, Sections 531 through 540a of Title 28, United States Code (U.S.C.), provide for the appointment of the Director and enumerate some of his powers. More importantly, with regard to promulgation of the DIOG, Section 301 of Title 5, U.S.C., authorizes the head of an Executive department to "prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property." The Attorney General, as head of the DOJ, has delegated the authority in Section 301 to the Director in a variety of orders and regulations. Foremost among these delegations are Subpart P and Section 0.137 of Title 28, Code of Federal Regulations (C.F.R.). This DIOG is promulgated under the authority thus delegated.

(U//FOUO) The Director's role and responsibilities under the AGG-Dom and DIOG, include, among others, the approval or denial of departures from the AGG-Dom, Undisclosed Participation (UDP) (see DIOG Section 16) and Sensitive Operations Review Committee (SORC) matters (see DIOG Section 10).

3.2.2 (U) DEPUTY DIRECTOR'S AUTHORITY, ROLES AND RESPONSIBILITY

(U//FOUO) The Deputy Director is the proponent of the DIOG, and in that position has oversight regarding compliance with the DIOG and subordinate implementing procedural directives and divisional specific PGs. The Deputy Director is also responsible for the development and the delivery of necessary training and the execution of the monitoring and auditing processes.

(U//FOUO) The Deputy Director works through the Corporate Policy Office (CPO) to ensure the following:

- A) (U//FOUO) The DIOG is updated as necessary to comply with changes in the law, rules, or regulations;

- B) (U//FOUO) The DIOG is reviewed every three years after the effective date of the 2011 revision, and revised as appropriate. This mandatory review schedule, however, does not restrict the CPO, which is responsible for all corporate policy matters, from working with FBI Headquarters (FBIHQ) divisions and field offices in the meantime to make policy revisions to the DIOG and the PGs whenever necessary and appropriate during the three year period. The CPO may also make technical or non-substantive language or formatting changes to the DIOG, as necessary, provided those changes clarify the meaning without altering the substance of the DIOG;
- C) (U//FOUO) Existing and proposed investigative and administrative policies and PGs comply with the standards established in the AGG-Dom and DIOG. On behalf of the Deputy Director, the CPO has the authority, following coordination with the OIC and OGC, to modify or remove any provision of existing or proposed investigative or administrative policies or PGs determined to violate, contradict, or otherwise modify the intent or purpose of any provision or standard established in the AGG-Dom or DIOG; and
- D) (U//FOUO) If the CPO makes any changes to the DIOG or other policy pursuant to DIOG Sections 3.2.2.B and/or 3.2.2.C above, the CPO will immediately advise by e-mail all FBIHQ and field office Division Policy Officers (DPO) of such changes and all DPOs must further advise their respective FBI employees of such changes. The electronic version of the DIOG maintained in the CPO's Policy and Guidance Library is the official current policy of the FBI.

3.3 (U) SPECIAL AGENT/INTELLIGENCE ANALYST/TASK FORCE OFFICER (TFO)/TASK FORCE MEMBER (TFM)/TASK FORCE PARTICIPANT (TFP)/FBI CONTRACTOR/OTHERS - ROLES AND RESPONSIBILITIES

3.3.1 (U) ROLES AND RESPONSIBILITIES

(U//FOUO) Special Agents, analysts, TFO, TFM, TFP, FBI contractors and others bound by the AGG-Dom and DIOG must:

3.3.1.1 (U) TRAINING

(U//FOUO) Obtain training on the DIOG standards relevant to his/her position and perform activities consistent with those standards;

3.3.1.2 (U) INVESTIGATIVE ACTIVITY

(U//FOUO) Ensure all investigative activity complies with the Constitution, Federal law, executive orders, Presidential Directives, AGG-Dom, other Attorney General Guidelines (AGG), Treaties, Memoranda of Agreement/Understanding, the DIOG, and any other applicable legal and policy requirements (if an agent, analyst, TFO, or other individual is unsure of the legality of any action, he/she must consult with his/her supervisor, the Chief Division Counsel (CDC) or OGC);

3.3.1.3 (U) PRIVACY AND CIVIL LIBERTIES

(U//FOUO) Ensure that civil liberties and privacy are protected throughout the Assessment or investigative process;

3.3.1.4 (U) PROTECT RIGHTS

(U//FOUO) Conduct no investigative activity based solely on the exercise of First Amendment activities (i.e., the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, national origin or religion of the subject (See DIOG Section 4);

3.3.1.5 (U) COMPLIANCE

(U//FOUO) Ensure compliance with the DIOG, including standards for opening, conducting, and closing an investigative activity; collection activity; or use of an investigative method, as provided in the DIOG;

3.3.1.6 (U) REPORT NON-COMPLIANCE

(U//FOUO) Comply with the law, rules, or regulations, and report any non-compliance concern to the proper authority. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see DIOG Sections 2.6 - 2.8;

3.3.1.7 (U) ASSIST VICTIMS

(U//FOUO) Identify victims who have suffered direct physical, emotional, or financial harm as result of the commission of Federal crimes, offer the FBI's assistance to victims of these crimes and provide victims' contact information to the responsible FBI Victim Specialist (VS). The VS is thereafter responsible for keeping victims updated on the status of the investigation to the extent permitted by law, regulation, or policy, unless the victim has opted not to receive assistance. The FBI's responsibility for assisting victims is continuous as long as there is an open investigation (see the Office of Victim Assistance PG);

3.3.1.8 (U) OBTAIN APPROVAL

(U//FOUO) Ensure appropriate supervisory approval is obtained for investigative activity as required in the DIOG. Obtain and document oral approval as specified in Section 3.4.2.2 below. Self-approval of DIOG activities is not permitted. See "No Self-Approval Rule" set forth in Section 3.4.2.3 below;

3.3.1.9 (U) ATTRIBUTE INFORMATION TO ORIGINATOR IN REPORTS

(U//FOUO) Ensure that if the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, FBI records (i.e., 302s, ECs, LHMs, etc.) reflect that another party, and not the FBI, is the originator of the characterization. Example: An FBI document should state: "The complainant advised that the subject was prejudiced and motivated by ethnic bias" rather than "The subject was prejudiced and motivated by ethnic bias;"

3.3.1.10 (U) SERVE AS INVESTIGATION ("CASE") MANAGER

(U//FOUO) If assigned responsibility for an investigation, manage all aspects of that investigation, until it is assigned to another person. It is the employee's responsibility to ensure compliance with all applicable laws, rules, regulations, and guidelines, both

investigative and administrative, from the opening of the investigation through disposition of the evidence, until the investigation is assigned to another person;

3.3.1.11 (U) CREATE AND MAINTAIN RECORDS/FILES

(U//FOUO) Create and maintain authentic, reliable, and trustworthy records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14 and Appendix J;

3.3.1.12 (U) INDEX DOCUMENTS

(U//FOUO) If assigned responsibility for an investigation, index information in documents. Current guidance for indexing documents may be found in DIOG Appendix J and on the RMD website: <http://home.fbinet.fbi/do/rmd/Pages/Default.aspx>;

3.3.1.13 (U) SEEK FEDERAL PROSECUTION

(U//FOUO) Prefer Federal prosecution rather than state/local prosecution. An FBI employee may protect the FBI's resources and interests when discussing investigations with the United States Attorney's Office (USAO) by accurately representing the time and effort spent on an investigation. The USAO should be aware of this information prior to deciding whether he/she will decline prosecution in favor of handling by local authorities. Criminal investigations conducted by the FBI are designed to obtain evidence for prosecution in Federal court and not in state or local courts; and

3.3.1.14 (U) RETAIN NOTES MADE DURING AN INVESTIGATION

(U//FOUO) Retain in the investigative file (1A envelope) the following types of material developed when interviewing witnesses:

- A) (U) Statements signed by the witness.
- B) (U) Written statements, unsigned by the witness, but approved or adopted in any manner by the witness.
- C) (U) Original notes of interview with prospective witnesses and/or suspects and subjects. That is, in any interview where preparation of an FD-302 is required (an interview where it is anticipated the results will become the subject of court testimony) the handwritten notes must be retained.
- D) (U) Dictating interview notes on audio tape in lieu of handwritten notes may be viewed by a court as "original notes" and, therefore, must be retained. Dictation on audio tape of the results of an interview for transcription to a final FD-302 is not "original note" material and need not be retained.
- E) (U) An FBI employee's notes made to record his/her own finding, must always be retained. Such notes include, but are not limited to, accountant's work papers and notes covering matters such as crime scene searches, laboratory examinations, and fingerprint examinations. If there is a question whether notes must be retained, resolve the question in favor of retaining the notes.

3.3.2 (U) DEFINITIONS OF TASK FORCE OFFICER (TFO), TASK FORCE MEMBER (TFM), AND TASK FORCE PARTICIPANT (TFP)

(U//FOUO) It is required in some situations for the sponsoring agency of the TFO, TFM and TFP to enter into an MOU with the FBI that governs the activities of the Task Force. For purposes of the DIOG, TFO, TFM, and TFP are defined as follows:

3.3.2.1 (U) TASK FORCE OFFICER (TFO)

(U//FOUO) An individual is a TFO when all of the following apply:

- A) (U//FOUO) The individual is a certified Federal, state, local, or tribal law enforcement officer;
- B) (U//FOUO) The individual is authorized to carry a firearm;
- C) (U//FOUO) The individual is currently deputized under either Title 21 or Title 18 of the U.S.C.;
- D) (U//FOUO) The individual has been issued Federal law enforcement credentials;
- E) (U//FOUO) The individual is assigned to the supervision of an FBI led task force;
- F) (U//FOUO) The individual has a security clearance recognized by the FBI that is currently active; and
- G) (U//FOUO) The individual is authorized to have access to FBI facilities.

(U//FOUO) An FBI TFO is mandated to attend all DIOG related training, and is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFO.

3.3.2.2 (U) TASK FORCE MEMBER (TFM)

(U//FOUO) An individual is a TFM when all of the following apply:

- A) (U//FOUO) The individual is an employee of a Federal, state, local, or tribal agency;
- B) (U//FOUO) The individual is assigned to the supervision of an FBI led task force;
- C) (U//FOUO) The individual has a security clearance recognized by the FBI that is currently active; and
- D) (U//FOUO) The individual is authorized to have access to FBI facilities.

(U//FOUO) An FBI TFM is mandated to attend all DIOG related training, and is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFM.

3.3.2.3 (U) TASK FORCE PARTICIPANT (TFP) (I.E., TASK FORCE LIAISON)

(U//FOUO) An individual is a TFP when he/she participates on an FBI-led task force and does not otherwise qualify as a TFO or TFM. A TFP is bound by all rules, regulations, and policies set forth in the DIOG when acting in the capacity as an FBI TFP. DIOG related training for an FBI TFP may be required by the head of the office/division that governs the activities of the Task Force.

3.4 (U) SUPERVISOR ROLES AND RESPONSIBILITIES

3.4.1 (U) SUPERVISOR DEFINED

(U) The term “supervisor” as used in the DIOG includes (whether in a Field Office or FBIHQ) the following positions, or a person acting in such capacity:

- A) (U) Supervisory Special Agent (SSA),
- B) (U) Supervisory Senior Resident Agent (SSRA),
- C) (U) Supervisory Intelligence Analyst (SIA),
- D) (U) Legal Attache (Legat),
- E) (U) Deputy Legal Attache (DLAT),
- F) (U) Unit Chief (UC),
- G) (U) Assistant Special Agent in Charge (ASAC),
- H) (U) Assistant Section Chief (ASC),
- I) (U) Section Chief (SC),
- J) (U) Special Agent in Charge (SAC),
- K) (U) Deputy Assistant Director (DAD),
- L) (U) Assistant Director (AD),
- M) (U) Assistant Director in Charge (ADIC),
- N) (U) Associate Executive Assistant Director (A/EAD),
- O) (U) Executive Assistant Director (EAD),
- P) (U) Associate Deputy Director (ADD), and
- Q) (U) Deputy Director (DD).

(U) The term “supervisor” is also intended to include any other FBI supervisory or managerial position that is not specifically listed above but is equal in rank and/or responsibility to these listed positions. (Note: TFOs/TFMs cannot be supervisors.)

3.4.2 (U) SUPERVISOR RESPONSIBILITIES

3.4.2.1 (U) APPROVAL/REVIEW OF INVESTIGATIVE OR COLLECTION ACTIVITIES

(U//FOUO) Anyone in a supervisory role who approves/reviews investigative or collection activity must determine whether the standards for opening, approving, conducting, and closing an investigative activity, collection activity or investigative method, as provided in the DIOG, have been satisfied.

3.4.2.2 (U) ORAL AUTHORITY / APPROVAL

(U//FOUO) Unless otherwise specified by the AGG-Dom or FBI policy, any authority/approval required in the DIOG necessary to conduct investigative activities may be granted orally by the appropriate approving official. Should such oral authorization be

granted, appropriate written documentation of the oral authorization must be documented by the FBI employee to the authorizing official as soon as practicable, but not more than five business days after the oral authorization. The effective date of any such oral authorization is the date on which the oral authority was granted, and that date and the name of the approving official must be included in the subsequent written documentation.

(U//FOUO) Supervisors are not permitted to self-approve investigative or intelligence collection activity or methods in assessments or investigations assigned to them as case agents or analysts. An independent evaluation and approval of these activities must be obtained including the opening and closing of any Assessment or Predicated Investigation. See Section 3.4.2.3 below.

3.4.2.3 (U) NO SELF-APPROVAL RULE

(U//FOUO) When approval/authority is required in the DIOG to open, utilize an investigative method, close, or perform any administrative requirement (i.e. initial paperwork to a file, perform a file review, etc.), an approving official (supervisor) may not “self-approve” his/her own work or activity. An independent evaluation and approval of these activities must be obtained, including the opening and closing of any Assessment or Predicated Investigation.

(U//FOUO) Example: An SSA/SIA properly designates a relief supervisor on the squad to act as the SSA/SIA while the supervisor is on leave. The relief SSA/SIA may not approve anything related to his/her own investigations/work because supervisors are not permitted to self-approve investigative or intelligence collection activity or methods in files assigned to themselves.

3.4.2.4 (U) ENSURE COMPLIANCE WITH U.S. REGULATIONS AND OTHER APPLICABLE LEGAL AND POLICY REQUIREMENTS

(U//FOUO) Supervisors must monitor and take reasonable steps to ensure that all investigative activity, collection activity and the use of investigative methods comply with the Constitution, Federal law, Executive Orders, Presidential Directives, AGG-Dom, other AGG, Treaties, Memoranda of Agreement/Understanding, the DIOG, and any other applicable legal and policy requirements.

3.4.2.5 (U) TRAINING

(U//FOUO) Supervisors must obtain training on the DIOG standards relevant to his/her position and then conform decisions to those standards. Supervisors must also take reasonable steps to ensure that all subordinates have received the required training on the DIOG standards and requirements relevant to the subordinate’s position.

3.4.2.6 (U) PROTECT CIVIL LIBERTIES AND PRIVACY

(U//FOUO) All supervisors must take reasonable steps to ensure that civil liberties and privacy are protected throughout the investigative process.

3.4.2.7 (U) REPORT COMPLIANCE CONCERNS

(U//FOUO) If a supervisor encounters a practice that does not comply, or appears not to comply, with the law, rules, or regulations, the supervisor must report that compliance concern to the proper authority and, when necessary, take action to maintain compliance. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see Sections 2.6 - 2.8.

3.4.2.8 (U) NON-RETALIATION POLICY

(U//FOUO) Supervisors must not retaliate or take adverse action against persons who raise compliance concerns. (See CPD 0032D, 02/11/2008 for non-retaliation policy)

3.4.2.9 (U) CREATE AND MAINTAIN RECORDS/FILES

(U//FOUO) Supervisors must ensure that FBI employees create and maintain authentic, reliable, and trustworthy records, establish files, set leads, supervise investigations, index documents, and retain and share information, as specified in DIOG Section 14.

3.4.3 (U) DELEGATION AND SUCCESSION IN THE FBI

(U//FOUO) The ability to exercise legal authority within the FBI through delegations of legal authority and orderly succession to positions of authority is set forth in the Succession and Delegation Policy.

3.4.3.1 (U) DELEGATION

(U//FOUO) As used in the DIOG, the term “delegation” refers to the conveyance of authority to another official (either by position or to a named individual). FBI legal authority is generally delegable one supervisory level unless expressly permitted, prohibited, or restricted by law, regulation, or policy. For example, an SAC may delegate his/her authority to approve Sensitive Investigative Matters (SIMs) to an ASAC, but the ASAC cannot further delegate this authority to an SSA. Delegations will continue in effect until modified, revoked, superseded, the position no longer exists, or the named individual vacates the position.

(U//FOUO) A supervisor may only delegate authority to another supervisor one level junior to himself or herself, unless specified otherwise (e.g., an ASAC may delegate authority to an SSA). SACs may, however, restrict delegations within their field offices, i.e., an SAC may prohibit ASACs from further delegating authorities that have been assigned to them.

(U//FOUO) SSAs and Supervisory Intelligence Analysts (SIA) cannot “delegate” their authority because they are the first level of supervisory responsibility; however, a relief supervisor may exercise the SSA’s authority when serving as the “acting” SSA (e.g., when the SSA is absent or unavailable). In the absence of the immediate approval authority, a supervisor at the same or higher level than that required may approve a particular activity (e.g., an Special Agent requests that his/her ASAC or SAC approve a Preliminary Investigation because the Agent’s SSA is on a temporary duty assignment).

3.4.3.2 (U) SUCCESSION: ACTING SUPERVISORY AUTHORITY

(U//FOUO) As used in the DIOG, the term “succession” refers to the process by which an official assumes the authorities and responsibilities of an existing position, typically when the incumbent is absent, unavailable, unable to carry out official responsibilities, or has vacated the position. A person who temporarily succeeds to a position is referred to as “acting” in that position.

(U//FOUO) The FBI follows the general rule, recognized in law, that employees properly designated as “acting” in a position exercise the full legal authorities of that position, unless specifically precluded by higher authority or by an applicable law, regulation, or policy. Accordingly, unless expressly precluded, any authority vested in an FBI supervisor pursuant to the DIOG may be exercised by someone who occupies that position in an acting status. An employee may be designated to an acting position either through a succession plan or ad hoc designation. See the FBI Succession and Delegation Policy for additional details.

3.4.3.3 (U) DOCUMENTATION

(U//FOUO) Delegations of authority as well as succession plans and ad hoc designations must be documented in writing and maintained in an appropriate administrative file whenever practicable, unless specifically required by the DIOG. An administrative file has been created to maintain documentation of delegations of authority and ad hoc designations (319W-HQ-A1487698-xx with the last two alpha characters designating particular field office, FBIHQ Division or Legat). An administrative file has also been created to maintain documentation of succession plans (319X-HQ-A1538387-XX with the last two alpha characters designating the particular field office, FBIHQ Division or Legat). Documentation of acting authority may take place subsequent to the actual ad hoc designation. For example, an SSA orally advises his principal relief supervisor that he/she has an emergency and will not be able to come into the office. The ad hoc designation of the relief supervisor as acting SSA can be documented upon the SSA’s return to the office. Failure to document an ad hoc designation does not invalidate the designation but may result in difficulty proving the appropriate exercise of authority if required to do so. (See Section 3.4.2.2 above concerning oral authorizations and related documentation requirements).

3.4.4 (U) FILE REVIEWS AND JUSTIFICATION REVIEWS**3.4.4.1 (U) OVERVIEW**

(U//FOUO) The file review is designed to ensure investigative and intelligence activities are progressing adequately and conducted in compliance with applicable statutes, regulations, and FBI/DOJ policies and procedures. As a management tool, the file review process has proven effective for operational program oversight, tracking investigative and intelligence collection progress, ensuring investigative focus, and reduction of risk.

(U//FOUO) Supervisory review of investigative files is especially important with regard to tracking the progress and development of new employees. It provides an opportunity for supervisors to guide employees on how properly to manage and document investigation files, and to use and document investigative methods, while emphasizing the importance of

compliance and recognition of risk. In addition, the file review process is an opportunity to begin to evaluate an employee's level of performance and to identify his/her strengths and weaknesses.

(U//FOUO) File reviews help supervisors to ensure their office is effectively supervising activities in its own territory and monitoring investigative activity carried out on their behalf in other field offices. For example, a supervisor may use a file review as a reasonable step to ensure the employee assigned an investigation has addressed all logical investigation in a timely manner, or to ensure the employee has successfully set necessary leads for other offices or other employees within his/her own office.

3.4.4.2 (U) TYPES OF FILES/INVESTIGATIONS REQUIRING FILE REVIEWS AND JUSTIFICATION REVIEWS

(U//FOUO) File reviews must be conducted for all Predicated Investigations, including investigations placed in "pending inactive" status, unaddressed work files, and Types 3 through 6 Assessments. Type 1 & 2 Assessments must have a 30 day justification reviews, as specified below.

3.4.4.3 (U) FREQUENCY OF FILE REVIEWS

(U//FOUO) Supervisors must adhere to the following timeframes for file reviews:

A) **(U//FOUO) 90 Days** – The supervisor must review the files for all investigations (including pending Predicated Investigations, pending inactive investigations, unaddressed work files, and Type 3 - 6 Assessments) assigned to each agent, Resident Agent, TFO, and IA every 90 calendar days.

1) **(U//FOUO) 30 Additional Days:** All documentation of the required reviews must be completed within 30 calendar days of the file review date.

B) **(U//FOUO) 60 Days** – The supervisor must review the files for all investigations (including pending Predicated Investigations, pending inactive investigations, unaddressed work files, and Type 3 - 6 Assessments) assigned to each probationary employee (agent and IA) every 60 calendar days.

1) **(U//FOUO) 30 Additional Days:** All documentation of the required reviews must be completed within 30 calendar days of the file review date.

3.4.4.4 (U) FREQUENCY OF JUSTIFICATION REVIEWS

(U//FOUO) In addition to file reviews, every 30 days supervisors must complete "justification reviews" for Type 1 & 2 Assessments, as specified below.

3.4.4.5 (U) DELEGATION OF FILE REVIEWS

(U//FOUO) Thorough, complete and well conducted file reviews are an important part of the compliance regime, provide valuable and needed information for purposes of evaluating the performance of employees, and are critical to the effective management of a squad. For those reasons, file reviews are an important duty and responsibility for Supervisors, and Supervisors are discouraged from routinely delegating these reviews. Because, however, conducting a file review is an important developmental opportunity for primary relief supervisors, file reviews

may be conducted by a duly designated acting supervisor or duly designated primary relief supervisor. Acting supervisors may conduct file reviews just as they would conduct any other supervisory duty while functioning in an acting capacity. Primary relief supervisors may conduct file reviews; however, when they do so, the next required file review must be conducted by a supervisor or duly designated acting supervisor. In other words, every other file review of any given investigative file must be conducted by a supervisor or duly designated acting supervisor. Acting supervisors may not review their own files under any circumstances. Acting supervisors must either reassign their investigations or have their investigations reviewed by another supervisor or an ASAC.

3.4.4.6 (U) FILE REVIEW REQUIREMENTS FOR PREDICATED INVESTIGATIONS & ASSESSMENTS

(U//FOUO) A file review or justification review must be: conducted in person or by telephone when necessary (e.g., FBI employee is TDY or in a remote Resident Agency (RA)); conducted in private; and documented as specified below.

(U//FOUO) The file review process requires the supervisor to review the investigative files assigned to the employee, discuss past progress and future objectives, and document that information on the Investigative Case Management (ICM) Case Review Sheet generated by ACS (commonly referred to as the “file review sheet”). Discussion and documentation must also include the progress of the investigation/Assessment since the previous file review and the projected work for the time period until the next file review.

(U//FOUO) When reviewing the employee’s assigned investigative files, the supervisor should consider the following:

- A) (U//FOUO) Whether subject(s) have been indexed in compliance with indexing guidelines;
- B) (U//FOUO) Whether statistical accomplishments, i.e., FD-515 and FD-542, have been entered within established timeframes;
- C) (U//FOUO) Whether evidence has been stored and disposed of properly and whether documentation has been completed according to evidence control policies;
- D) (U//FOUO) Whether leads have been covered within established deadlines;
- E) (U//FOUO) Whether any National Security Letters have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);
- F) (U//FOUO) Whether any Federal Grand Jury Subpoenas have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);
- G) (U//FOUO) Whether any Administrative Subpoenas have been issued in accordance with policy, including whether responsive materials have been appropriately examined (e.g., examined for overproduction);
- H) (U//FOUO) Whether any Federal Grand Jury Materials covered by Rule 6e are properly marked and handled, including being appropriately restricted in ACS;
- I) (U//FOUO) Whether the Watchlist status of any subject(s) has been appropriately documented;

- J) (U//FOUO) Whether the status of the Preliminary Investigation is current (e.g., has not expired or will not expire before the next file review);
- K) (U//FOUO) Whether any Potential Intelligence Oversight Board (IOB) violations have been reported in accordance with policy; and
- L) (U//FOUO) Whether relevant asset forfeiture statutes have been applied and their use documented.

(U//FOUO) Supervisors must evaluate the proper use of investigative methods and ensure they are appropriately documented in the file. Leads and administrative actions must be documented in ECs. When evidence has been recovered, the supervisor must review all FD-192s to ensure the evidence was handled appropriately. The supervisor should use the file review process as an opportunity to determine whether the employee has adequately used liaison and external contacts to further the investigation/Assessment. In addition, the supervisor must assess whether the employee needs additional assistance, training, guidance, or other resources to successfully advance the investigation/Assessment.

(U//FOUO) The intelligence aspect of every investigation must be scrutinized during the file review process. The supervisor must determine whether the employee understands his/her responsibilities relative to intelligence collection and reporting and has ensured that investigative and intelligence aspects of each investigation complement each other. This includes examining whether the employee has adequately collaborated with the field office's intelligence component and exploited his/her investigations to obtain information relevant to standing intelligence collection requirements. The supervisor must review the files for potential intelligence collection and sharing opportunities, both cross-programmatic and interagency. The file review must document whether applicable intelligence products such as intelligence reports, bulletins and assessments, etc., have been or should be drafted based on investigative and intelligence information collected during the investigation.

(U//FOUO) The supervisor must also evaluate whether the employee has been in communication with FBIHQ division entities, if appropriate, with respect to his/her investigative/intelligence activities. The supervisor must also evaluate whether the employee has coordinated with FBIHQ to obtain any special authorities/concurrences needed from DOJ/FBI components and other governmental agencies (e.g., CIA, DOS, and DOD).

(U//FOUO) The supervisor must consider and take into account the employee's collateral duties, such as SWAT, ERT, HAZMAT, Hostage Negotiator, training, TDY assignments and other activities constituting official business that could limit his/her ability to address his/her assigned caseload. The supervisor must take into account planned annual and sick leave, holidays and similar time constraints when estimating the employee's overall work responsibilities for the next 90 day period.

(U//FOUO) The supervisor must evaluate whether the employee is acting within all applicable statutes, regulations, and FBI/DOJ policies and procedures. Supervisors must keep in mind that how the employee accomplishes his or her tasks is just as important as whether he or she accomplishes them. Any compliance concerns must be immediately referred to the field office's compliance officer for discussion regarding what additional actions should be taken. For specific requirements and procedures for reporting departures and non-compliance with the AGG-Dom and the DIOG, see Sections 2.6 - 2.8.

(U//FOUO) At the conclusion of the file review, the supervisor must ensure that the employee understands the objectives to be accomplished over the next 90 calendar days and must document specifically those expectations on the file review sheets. At this time the supervisor must also prepare an FD-865 (Performance Summary Assessment) for Special Agents per Corporate Policy Notice (CPN) 0043N. For all other employees, the supervisor has the option to prepare an FD-865.

(U//FOUO) The supervisor must be diligent about documenting all aspects of the file review on the file review sheet and setting appropriate ticklers.

3.4.4.7 (U) TYPE 1 & 2 ASSESSMENTS - JUSTIFICATION REVIEWS

(U//FOUO) Supervisors must conduct 30-day justification reviews for Type 1 & 2 Assessments. Following the end of the 30-day period, the agent, TFO, or IA and the supervisor have up to 10 calendar days to complete all aspects of the justification review and to document the review. These justification reviews must address the following Assessment Review Standards (ARS):

- A) (U//FOUO) has progress been made toward achieving the authorized purpose and clearly defined objective(s);
- B) (U//FOUO) were the activities that occurred in the prior 30 calendar days appropriate and in compliance with applicable DIOG requirements;
- C) (U//FOUO) is it reasonably likely that information will be obtained that is relevant to the authorized purpose and clearly defined objective(s), thereby warranting an extension for another 30 calendar days;
- D) (U//FOUO) has adequate predication been developed to open a Predicated Investigation; and
- E) (U//FOUO) should the Assessment be terminated.

(U//FOUO) The justification review, including the ARS requirements, must be documented in the FD-71 or the FD-71a (Guardian).

3.4.4.8 (U) TYPE 3, 4, AND 6 ASSESSMENTS - ASSESSMENT REVIEW STANDARDS (ARS)

(U//FOUO) In addition to the file review procedures documented on the File Review Sheet set forth above, supervisors are required to evaluate Type 3, 4 and 6 Assessments using the below- listed ARS during the file review every 90 calendar days (60 calendar days for probationary employees):

- A) (U//FOUO) has progress been made toward achieving the authorized purpose and clearly defined objective(s);
- B) (U//FOUO) were the activities that occurred in the prior 60 or 90 calendar days appropriate and in compliance with applicable DIOG requirements;
- C) (U//FOUO) is it reasonably likely that information may be obtained that is relevant to the authorized purpose and clearly defined objective(s), thereby warranting an extension for another 60/90 calendar days;
- D) (U//FOUO) has adequate predication been developed to open a Predicated Investigation on specific individuals identified during the Assessment; and

E) (U//FOUO) should the Assessment be terminated.

(U//FOUO) The ARS must be documented in an EC and uploaded to the Assessment file.

(U//FOUO) The EC utilized to document the review of Type 3, 4 and 6 Assessments must be made part of the Assessment file. Therefore, the EC must not be used to memorialize other information, such as performance measures, investigative steps, possible outcomes, or compliance matters that are historically documented on the File Review Sheet.

3.4.4.9 (U) TYPE 5 ASSESSMENTS - ASSESSMENT REVIEW STANDARDS (ARS)

(U//FOUO) In addition to the applicable file review procedures discussed above, supervisors are required to evaluate Type 5 Assessments using the below-listed ARS during the file review every 90 calendar days (60 days for probationary employees):

- A) (U//FOUO) whether authorized investigative methods have been used properly in all phases of the Assessment;
- B) (U//FOUO) whether, in the identification phase, the Assessment has successfully narrowed the field to a group of individuals who are likely to have appropriate placement and access;
- C) (U//FOUO) whether reimbursable expenses incurred by an SA, if any, were reasonable, properly authorized, and properly documented;
- D) (U//FOUO) whether the Potential CHS was “tasked” to provide information or paid for his/her services or expenses (activities which are not permitted prior to opening the person as a CHS);
- E) (U//FOUO) whether there is a reasonable likelihood that the Potential CHS can and should be recruited or, if the Assessment is in the Identification Phase, the plan has a reasonable likelihood of generating a group of Potential CHSs; and
- F) (U//FOUO) whether the Type 5 Assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is justified, the SIA/SSA must document the rationale for keeping the Type 5 Assessment open.

(U//FOUO) The review must be documented in an EC or successor form in DELTA and uploaded to the Assessment file. Because Type 5 Assessments are confidential, a Case Review Sheet is not available in ACS.

(U//FOUO) The EC (or successor form in DELTA) utilized to document the evaluation of the ARSs for Type 5 Assessments must be made part of the Assessment file. Therefore, the EC (or successor form in DELTA) must not be used to memorialize other information, such as performance measures, investigative steps, possible outcomes, or compliance matters.

3.4.4.10 (U) DOCUMENTATION OF FILE REVIEWS

(U//FOUO) Investigative Case Management (ICM) Case Review Sheets (also known as File Review Sheets) are currently generated by ACS. These must be completed by the supervisor as part of the file review process and maintained as a part of the employee’s performance folder to be used as a tool in determining an employee’s performance rating. Documents maintained for evaluations, including copies of File Review Sheets, must be destroyed within 30 calendar days after the expiration of the previous PAR year. The original File Review Sheets are to be maintained for inspection and other purposes not related to the performance appraisal process (FBI Corporate Policy Notice 0043N).

(U//FOUO) Performance Summary Assessments (PSA) are required to be completed by the supervisor as part of the file review process (see FBI Corporate Policy Notice 0043N). The FD-865 must be used to memorialize the PSA. The form must be signed and dated by the supervisor. The original FD-865 must be submitted to the field office's executive management, which is responsible for ensuring that PSAs are conducted. One completed copy of the FD-865 must be placed in the employee's performance folder maintained by the rating official for inspection, mid-year progress reviews, development worksheets, and annual performance appraisal purposes (this provision does not apply to TFOs). A second completed copy must be given to the employee. FD-865s maintained for performance evaluation must be destroyed within 30 calendar days after the expiration of the previous Performance Annual Review (PAR) year.

3.4.4.11 (U) RECORDS RETENTION

(U//FOUO) Supervisors must conduct, document and retain file reviews as specified above. Supervisors must maintain appropriate documentation and review it periodically with particular attention to documenting an employee's ability to successfully complete his or her investigative assignments and to documenting a probationary employee's success or failure during the probationary period.

3.5 (U) CHIEF DIVISION COUNSEL (CDC) ROLES AND RESPONSIBILITIES

(U//FOUO) The CDC must review all Assessments and Predicated Investigations involving sensitive investigative matters as discussed in DIOG Section 10 as well as review the use of certain investigative methods as discussed in Section 18. The primary purpose of the CDC's review is to ensure the legality of the actions proposed. Review, in this context, includes a determination that the investigative activity is: (i) not legally objectionable (e.g., that it is not based solely on the exercise of First Amendment rights (i.e., the free exercise of speech, religion, assembly, press or petition) or on the race, ethnicity, national origin or religion of the subject); and (ii) founded upon an authorized purpose and/or adequate factual predication and meets the standard specified in the DIOG. The CDC should also include in his or her review and recommendation, if appropriate, a determination of the wisdom of the proposed action (e.g., the CDC may have no legal objection but may recommend denial because the value of the proposal is outweighed by the intrusion into legitimate privacy interests). The CDC's determination that an investigative activity is: (i) not legally objectionable; and (ii) warranted from a mission standpoint is based on facts known at the time of the review and recommendation. Often, these facts are not verified or otherwise corroborated until the investigative activity commences. As a result, the CDC may require additional CDC reviews or provide guidance to supervisory personnel with regard to monitoring the results of the investigative activity to ensure that the authorized purpose and/or factual predication remains intact after the facts are developed. The regularity of such review is within the CDC's discretion. Activities found to be legally objectionable by the CDC may not be approved unless and until the CDC's determination is countermanded by the FBI General Counsel or a delegated designee.

(U//FOUO) For investigative activities involving a sensitive investigative matter, the CDC must also independently consider the factors articulated in Section 10 and provide the approving

authority with a recommendation as to whether, in the CDC's judgment, the investigative activity should be approved.

(U//FOUO) Throughout the DIOG, any requirement imposed on the CDC may be performed by an Associate Division Counsel (ADC) or a designated Acting CDC.

3.6 (U) OFFICE OF THE GENERAL COUNSEL (OGC) ROLES AND RESPONSIBILITIES

(U//FOUO) The mission of the FBI's Office of the General Counsel (OGC) is to provide comprehensive legal advice to the Director, other FBI officials and divisions, and field offices on a wide array of national security, investigative, and administrative operations. In addition to providing legal advice as requested, OGC reviews the legal sufficiency of sensitive Title III affidavits and a wide variety of operational documents relating to foreign counterintelligence/international terrorism investigations, including requests for surveillance and physical searches pursuant to the Foreign Intelligence Surveillance Act (FISA) and undercover proposals, and manages the physical flow of FISA requests, applications, orders, and returns. OGC maintains liaison with the intelligence community on legal issues and reviews for legal sufficiency proposals to share information or form partnerships with other federal, state, local, and international agencies. OGC also supports federal criminal prosecutions by assisting in criminal discovery and by conducting reviews of personnel files, coordinates the defense of the FBI and its employees in civil actions which arise out of the FBI's investigative mission and personnel matters, and responds to Congressional requests for FBI documents. OGC addresses legal issues associated with the impact of communication and information technology on the ability of the FBI and other law-enforcement and intelligence agencies to execute their public safety and national security missions, including their ability to conduct authorized electronic surveillance.

(U//FOUO) In coordination with the DOJ NSD, the OGC is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. The primary purpose of the OGC's review is to ensure the legality of the actions proposed. These reviews, conducted at FBI field offices and FBIHQ units, broadly examine such activities for compliance with the AGG-Dom and other applicable requirements. Review, in this context, includes a determination that the investigative activity is: (i) not legally objectionable (e.g., that it is not based solely on the exercise of First Amendment rights or on the race, ethnicity, national origin or religion of the subject); and (ii) founded upon an authorized purpose and/or adequate factual predication and meets the standard specified in the DIOG. The OGC should also include in its review and recommendation, if appropriate, a determination of the wisdom of the proposed action (e.g., the OGC may have no legal objection but may recommend denial because the value of the proposal is outweighed by the intrusion into legitimate privacy interests). The OGC's determination that an investigative activity is: (i) not legally objectionable; and (ii) warranted from a mission standpoint is based on facts known at the time of the review and recommendation. Often these facts are not verified or otherwise corroborated until the investigative activity commences. As a result, the OGC may require additional OGC reviews or provide guidance to supervisory personnel with regard to monitoring the results of the investigative activity to ensure that the authorized purpose and/or factual predication remains intact after the facts are developed. The regularity of such review is within the discretion of OGC.

(U//FOUO) For those investigative activities involving a sensitive investigative matter requiring OGC review, the OGC must independently consider the factors articulated in Section 10 and provide the approving authority with a recommendation as to whether, in the OGC's judgment, the investigative activity should be approved.

(U//FOUO) Throughout the DIOG, any requirement imposed on the General Counsel may be delegated and performed by a designated OGC attorney. All delegations must be made as set forth in Section 3.4.3 above.

3.7 (U) CORPORATE POLICY OFFICE (CPO) ROLES AND RESPONSIBILITIES

(U//FOUO) Subject to the guidance of the Deputy Director, the CPO has oversight of the implementation of the DIOG. Working with the Deputy Director's office, the CPO may make revisions to the DIOG as necessary, following appropriate coordination with the OIC, OGC and other FBIHQ or field office entities. In the process of implementing and analyzing the DIOG, the CPO should report any apparent compliance risk areas directly to the OIC. Additionally, the CPO will work directly with the OIC to ensure that the policies, training and monitoring are adequate to meet compliance monitoring procedures.

(U//FOUO) The CPO is responsible for ensuring the following:

- A) (U//FOUO) The DIOG is updated as necessary to comply with changes in the law, rules, or regulations;
- B) (U//FOUO) The DIOG is reviewed every three years from the effective date of the 2011 revision, and revised as appropriate. This mandatory review schedule, however, does not restrict the CPO, which is responsible for all corporate policy matters, from working with FBIHQ divisions and field offices to make policy revisions to the DIOG and the PGs whenever necessary and appropriate during the three year period. The CPO may also make technical or non-substantive language or formatting changes to the DIOG, as necessary, provided those changes clarify the meaning without altering the substance;
- C) (U//FOUO) Existing and proposed investigative and administrative policies and PGs comply with the standards established in the AGG-Dom and DIOG. On behalf of the Deputy Director, the CPO has the authority, following coordination with the OIC and OGC, to modify or remove any provision of existing or proposed investigative or administrative policies or PGs determined to violate, contradict, or otherwise modify the intent or purpose of any provision or standard established in the AGG-Dom or the DIOG; and
- D) (U//FOUO) If the CPO makes any changes to the DIOG or other policy pursuant to 3.7.B and/or C above, the CPO will immediately advise by e-mail all FBIHQ and field office Division Policy Officers (DPO) of such changes and all DPO must further advise their respective FBI employees of such changes. The electronic version of the DIOG maintained in the CPO's Policy and Guidance Library is the official current policy of the FBI.

3.8 (U) OFFICE OF INTEGRITY AND COMPLIANCE (OIC) ROLES AND RESPONSIBILITIES

(U//FOUO) OIC is responsible for reviewing the DIOG and working with each FBIHQ division and the CPO to identify compliance risk areas and to ensure the adequacy of policy statements, training and monitoring. When compliance risk areas are identified, OIC must work with the

divisions, field offices, and/or programs affected by the risk and develop programs to review the adequacy of policy statements, training, and monitoring in order to mitigate those concerns appropriately.

3.9 (U) OPERATIONAL PROGRAM MANAGER ROLES AND RESPONSIBILITIES

(U//FOUO) In addition to managing national level programs, coordinating investigations, training, and providing guidance and oversight to the field, the FBIHQ Operational Program Managers are responsible for identifying, prioritizing, and analyzing potential compliance risks within their programs regarding implementation of the DIOG and developing mitigation plans where warranted.

(U//FOUO) Operational Program Managers must proactively identify and take appropriate action to resolve potential compliance concerns. In identifying possible compliance concerns, Program Managers should consider the following indicators of possible compliance issues:

- A) (U//FOUO) Similar activities being handled differently from squad-to-squad / unit-to-unit / field office-to-field office;
- B) (U//FOUO) Unusually high level of contact with FBIHQ' division for basic information on how to conduct an activity;
- C) (U//FOUO) Apparent confusion over how to conduct a certain activity;
- D) (U//FOUO) Policy conflict;
- E) (U//FOUO) Non-existent/inaccurate/wrongly targeted training;
- F) (U//FOUO) Monitoring mechanisms that do not exist or do not test the right information (e.g. file reviews/program management); and
- G) (U//FOUO) Inadequate processes in place to audit for compliance.

(U//FOUO) Operational Program Managers may not retaliate or take adverse action against persons who raise compliance concerns.

3.10 (U) DIVISION COMPLIANCE OFFICER ROLES AND RESPONSIBILITIES

(U//FOUO) Each FBIHQ division and field office must have a Division Compliance Officer (DCO). The DCO will proactively identify potential risk of non-compliance in the implementation of the DIOG and report them to the proper authority and the OIC. The DCO must always be aware that the focus of a compliance program is the identification and resolution of a compliance problem using non-punitive and non-retaliatory means.

3.11 (U) POSITION EQUIVALENTS - FBI HEADQUARTERS (FBIHQ) APPROVAL LEVELS

(U//FOUO) The official position equivalents between the field offices and FBIHQ are outlined below. In general, an equivalent position at either the field or FBIHQ may exercise DIOG authority, unless the DIOG specifically limits a given authority. The equivalent positions are:

- A) (U//FOUO) Field Office Analyst or Special Agent = FBIHQ Analyst or Special Agent;

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§3

- B) (U//FOUO) Field Office SIA = FBIHQ SIA;
- C) (U//FOUO) CDC = FBIHQ OGC General Attorney;
- D) (U//FOUO) Field Office SSA = FBIHQ SSA;
- E) (U//FOUO) Field Office ASAC = FBIHQ UC;
- F) (U//FOUO) SAC = FBIHQ SC; and
- G) (U//FOUO) ADIC = FBIHQ AD.

4 (U) PRIVACY AND CIVIL LIBERTIES, AND LEAST INTRUSIVE METHODS

4.1 (U) CIVIL LIBERTIES AND PRIVACY

4.1.1 (U) OVERVIEW

(U) The FBI is responsible for protecting the security of our nation and its people from crime and terrorism while maintaining rigorous obedience to the Constitution. *The Attorney General's Guidelines for Domestic FBI Activities* (AGG-Dom) establish a set of basic principles that serve as the foundation for all FBI mission-related activities. When these principles are applied, they demonstrate respect for civil liberties and privacy as well as adherence to the Constitution and laws of the United States. These principles are as follows:

- A) (U) **Protecting the public includes protecting their rights and liberties.** FBI investigative activity is premised upon the fundamental duty of government to protect the public, which must be performed with care to protect individual rights and to ensure that investigations are confined to matters of legitimate government interest.
- B) (U) **Only investigate for a proper purpose.** All FBI investigative activity must have an authorized law enforcement, national security, or foreign intelligence purpose.
- C) (U) **Race, ethnicity, religion, or national origin alone can never constitute the sole basis for initiating investigative activity.** Although these characteristics may be taken into account under certain circumstances, there must be an independent authorized law enforcement or national security purpose for initiating investigative activity.
- D) (U) **Only perform authorized activities in pursuit of investigative objectives.** Authorized activities conducted as part of a lawful assessment or investigation include the ability to: collect criminal and national security information, as well as foreign intelligence; provide investigative assistance to federal, state, local, tribal, and foreign agencies; conduct intelligence analysis and planning; and retain and share information.
- E) (U) **Employ the least intrusive means that do not otherwise compromise FBI operations.** Assuming a lawful intelligence or evidence collection objective, i.e., an authorized purpose, strongly consider the method (technique) employed to achieve that objective that is the least intrusive available (particularly if there is the potential to interfere with protected speech and association, damage someone's reputation, intrude on privacy, or interfere with the sovereignty of foreign governments) while still being operationally sound and effective.
- F) (U) **Apply best judgment to the circumstances at hand to select the most appropriate investigative means to achieve the investigative goal.** The choice of which investigative method to employ is a matter of judgment, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom when the degree of intrusiveness is warranted in light of the seriousness of the matter concerned.

4.1.2 (U) PURPOSE OF INVESTIGATIVE ACTIVITY

(U) One of the most important safeguards in the AGG-Dom—one that is intended to ensure that FBI employees respect the constitutional rights of Americans—is the threshold requirement that

all investigative activities be conducted for an authorized purpose. Under the AGG-Dom that authorized purpose must be an authorized national security, criminal, or foreign intelligence collection purpose.

(U) Simply stating such a purpose, however, is not sufficient to ensure compliance with this requirement. The authorized purpose must be well-founded and well-documented. In addition, the information sought and the investigative method used to obtain it must be focused in scope, time, and manner to achieve the underlying purpose. Furthermore, the Constitution sets limits on what that purpose may be. It may not be solely to monitor the exercise of constitutional rights, such as the free exercise of speech, religion, assembly, press and petition, and, equally important, the authorized purpose may not be based solely on the race, ethnicity, national origin or religious beliefs of an individual, group, or organization or a combination of only those factors.

(U) It is important to understand how the “authorized purpose” requirement and these constitutional limitations relate to one another. For example, individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, or promoting certain religious beliefs—have a First Amendment right to do so. No investigative activity may be conducted for the sole purpose of monitoring the exercise of these rights. If a well-founded basis to conduct investigative activity exists, however, and that basis is not solely activity that is protected by the First Amendment or on the race, ethnicity, national origin or religion of the participants—FBI employees may assess or investigate these activities, subject to other limitations in the AGG-Dom and the DIOG. In such a situation, the investigative activity would not be based solely on constitutionally-protected conduct or on race, ethnicity, national origin or religion. Finally, although investigative activity would be authorized in this situation, it is important that it be conducted in a manner that does not materially interfere with the ability of the individuals or groups to engage in the exercise of constitutionally-protected rights.

4.1.3 (U) OVERSIGHT AND SELF-REGULATION

(U) Every FBI employee has the responsibility to ensure that the activities of the FBI are lawful, appropriate and ethical as well as effective in protecting the civil liberties and privacy of individuals in the United States. Strong oversight mechanisms are in place to assist the FBI in carrying out this responsibility. Department of Justice (DOJ) oversight is provided through provisions of the AGG-Dom, other Attorney General Guidelines, and oversight by other DOJ components. DOJ and the FBI’s Inspection Division, and the FBI’s Office of Integrity and Compliance (OIC) and Office of the General Counsel (OGC), also provide substantial monitoring and guidance. In the criminal investigation arena, prosecutors and district courts exercise oversight of FBI activities. In the national security and foreign intelligence arenas, the DOJ National Security Division (NSD) exercises that oversight. The DOJ NSD’s Oversight Section and the FBI’s OGC are responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews, conducted at FBI field offices and FBI Headquarters (FBIHQ) divisions, broadly examine such activities for compliance with the AGG-Dom and other applicable requirements. In addition, the AGG-Dom creates additional requirements, including:

- A) (U) Required notification by the FBI to the DOJ NSD concerning a Full Investigation that involves foreign intelligence collection, a Full Investigation of a United States person

(USPER) in relation to a threat to the national security, or a national security investigation involving a “sensitive investigative matter” (SIM) (see DIOG Section 10).

- B) (U) An annual report by the FBI to the DOJ NSD concerning the FBI’s foreign intelligence collection program, including information reflecting the scope and nature of foreign intelligence collection activities in each FBI field office.
- C) (U) Access by the DOJ NSD to information obtained by the FBI through national security or foreign intelligence activities.
- D) (U) General authority for the Assistant Attorney General for National Security to obtain reports from the FBI concerning these activities. (AGG-Dom, Intro. C)

(U) Further examples of oversight mechanisms include the involvement of both FBI and prosecutorial personnel in the review of undercover operations involving sensitive circumstances; notice requirements for investigations involving sensitive investigative matters; and notice and oversight provisions for Enterprise Investigations, which involve a broad examination of groups implicated in criminal and national security threats. These requirements and procedures help to ensure that the rule of law is respected in the FBI’s activities and that public confidence is maintained in these activities. (AGG-Dom, Intro. C)

(U) In addition to the above-described oversight mechanisms, the FBI is subject to a regime of oversight, legal limitations, and self-regulation designed to ensure strict adherence to the Constitution. This regime is comprehensive and has many facets, including the following:

- A) (U) The Foreign Intelligence Surveillance Act of 1978, as amended, and Title III of the Omnibus Crime Control and Safe Streets Act of 1968. These laws establish the processes for obtaining judicial approval of electronic surveillance and physical searches for the purpose of collecting foreign intelligence and electronic surveillance for the purpose of collecting evidence of crimes.
- B) (U) The Whistleblower Protection Acts of 1989 and 1998. These laws protect whistleblowers from retaliation.
- C) (U) The Freedom of Information Act of 1966. This law provides the public with access to FBI documents not covered by a specific statutory exemption.
- D) (U) The Privacy Act of 1974. This law balances the government’s need to maintain information about United States citizens and legal permanent resident aliens with the rights of those individuals to be protected against unwarranted invasions of their privacy stemming from the government’s collection, use, maintenance, and dissemination of that information. The Privacy Act forbids the FBI and other federal agencies from collecting information about how individuals exercise their First Amendment rights, unless that collection is expressly authorized by statute or by the individual, or is pertinent to and within the scope of an authorized law enforcement activity (5 U.S.C. § 552a[e][7]). Activities authorized by the AGG-Dom – with the exception of Positive Foreign Intelligence collection (see DIOG Section 9.3) – are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act.
- E) (U) Documents describing First Amendment activity that are subsequently determined to have been collected or retained in violation of the Privacy Act must be destroyed as set forth in Records Management Division (RMD) Policy Notice 0108N.

(U) Congress, acting primarily through the Judiciary and Intelligence Committees, exercises regular, vigorous oversight into all aspects of the FBI’s operations. To this end, the National

Security Act of 1947 requires the FBI to keep the intelligence committees (for the Senate and House of Representatives) fully and currently informed of substantial intelligence activities. This oversight has significantly increased in breadth and intensity since the 1970's, and it provides important additional assurance that the FBI conducts its investigations according to the law and the Constitution. Advice on what activities fall within the supra of required congressional notification can be obtained from OCA [A Corporate Policy Directive is forthcoming].

(U) The FBI's intelligence activities (as defined in Section 3.4(e) of Executive Order (EO) 12333 [see DIOG Appendix B]) are subject to significant self-regulation and oversight beyond that conducted by Congress. The Intelligence Oversight Board (IOB), comprised of members from the President's Intelligence Advisory Board (PIAB), also conducts oversight of the FBI's intelligence activities. Among its responsibilities, the IOB must inform the President of intelligence activities the IOB believes: (i)(a) may be unlawful or contrary to EO or Presidential Decision Directive (PDD), and (b) are not being adequately addressed by the Attorney General, the Director of National Intelligence (DNI), or the head of the department concerned; or (ii) should be immediately reported to the President. The requirements and procedures for reporting potential IOB matters to OGC/NSLB can be found in Corporate Policy Directive 0188D (Guidance on IOB Matters), and the Policy Implementation Guide (PG) 0188PG.

(U) Internal FBI safeguards include:

- A) (U) the OGC's Privacy and Civil Liberties Unit (PCLU), which reviews plans for any proposed FBI record system for compliance with the Privacy Act and related privacy protection requirements and policies and which provides legal advice on civil liberties questions;
- B) (U) the criminal and national security undercover operations review committees, comprised of senior DOJ and FBI officials, which review all proposed undercover operations that involve sensitive circumstances;
- C) (U) the Sensitive Operations Review Committee (SORC), comprised of senior DOJ and FBI officials, which provides oversight of those investigative activities that may impact civil liberties and privacy and that are not otherwise subject to high level FBI and DOJ review;
- D) (U) the FBI requirement that all FBI employees report departures from and non-compliance with the DIOG to their supervisor, other management officials, or appropriate authorities as set forth in DIOG Sections 2.6 – 2.8 and 3.1.1; and
- E) (U) training new FBI employees on privacy and periodic training for all FBI employees to maintain currency on the latest guidelines, changes to laws and regulations, and judicial decisions related to constitutional rights and liberties.

4.2 (U) PROTECTION OF FIRST AMENDMENT RIGHTS

(U) A fundamental principle of the Attorney General's Guidelines for FBI investigations and operations since the first guidelines were issued in 1976 has been that investigative activity may not be based solely on the exercise of rights guaranteed by the First Amendment to the United States Constitution. This principle carries through to the present day in the AGG-Dom. The Privacy Act contains a corollary principle – the government is prohibited from retaining information describing how a person exercises rights under the First Amendment, unless that

information is pertinent to or within the scope of an authorized law enforcement activity. 5 U.S.C. § 552a(e)(7).

(U) The First Amendment states:

(U) Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

(U) Although the amendment appears literally to apply only to Congress, the Supreme Court made clear long ago that it also applies to activities of the Executive Branch, including law enforcement agencies. Therefore, for FBI purposes, it would be helpful to read the introduction to the first sentence as: “The FBI shall take no action respecting...” In addition, the word “abridging” must be understood. “Abridging,” as used here, means “diminishing.” Thus, it is not necessary for a law enforcement action to destroy or totally undermine the exercise of First Amendment rights for it to be unconstitutional; significantly diminishing or lessening the ability of individuals to exercise these rights without an authorized investigative purpose is sufficient.

(U) This is not to say that any diminution of First Amendment rights is unconstitutional. The Supreme Court has never held that the exercise of these rights is absolute. In fact, the Court has realistically interpreted the level and kind of government activity that violates a First Amendment right. For example, taken to an extreme, one could argue that the mere possibility of an FBI agent being present at an open forum (or as an on-line presence) would diminish the right of free speech by a participant in the forum because he/she would be afraid to speak freely. The Supreme Court, however, has never found an “abridgement” of First Amendment rights based on such a subjective fear. Rather, the Court requires an action that, from an objective perspective, truly diminishes the speaker’s message or his/her ability to deliver it (e.g., pulling the plug on the sound system). For another example, requiring protestors to use a certain parade route may diminish their ability to deliver their message in a practical sense, but the Court has made it clear, that for legitimate reasons (e.g., public safety), the government may impose reasonable limitations in terms of time, place and manner on the exercise of such rights, as long as the ability to deliver the message remains.

(U) While the language of the First Amendment prohibits action that would abridge the enumerated rights, the implementation of that prohibition in the AGG-Dom reflects the Supreme Court’s opinions on the constitutionality of law enforcement action that may impact the exercise of First Amendment rights. As stated above, the AGG-Dom prohibits investigative activity for the sole purpose of monitoring the exercise of First Amendment rights. The importance of the distinction between this language and the actual text of the First Amendment is two-fold: (i) the line drawn by the AGG-Dom prohibits even “monitoring” the exercise of First Amendment rights (far short of abridging those rights) as the sole purpose of FBI activity; and (ii) the requirement of an authorized purpose for all investigative activity provides additional protection for the exercise of constitutionally protected rights.

(U) The AGG-Dom classifies investigative activity that involves a religious or political organization (or an individual prominent in such an organization) or a member of the news media as a “sensitive investigative matter.” That designation recognizes the sensitivity of conduct that traditionally involves the exercise of First Amendment rights by groups, e.g., who

associate for political or religious purposes or by the press. The requirements for opening and pursuing a “sensitive investigative matter” are set forth in DIOG Section 10. It should be clear, however, from the discussion below just how pervasive the exercise of First Amendment rights is in American life and that not all protected First Amendment activity will fall within the definition of a “sensitive investigative matter.” Therefore, it is essential that FBI employees recognize when investigative activity may have an impact on the exercise of these fundamental rights and be especially sure that any such investigative activity has a valid law enforcement or national security purpose, even if it is not a “sensitive investigative matter” as defined in the AGG-Dom and the DIOG.

(U) Finally, it is important to note that individuals in the United States (and organizations comprised of such individuals) do not forfeit their First Amendment rights simply because they also engage in criminal activity or in conduct that threatens national security. For example, an organization suspected of engaging in acts of domestic terrorism may also pursue legitimate political goals and may also engage in lawful means to achieve those goals. The pursuit of these goals through constitutionally protected conduct does not insulate them from legitimate investigative focus for unlawful activities—but the goals and the pursuit of their goals through lawful means remain protected from unconstitutional infringement.

(U) When allegations of First Amendment violations are brought to a court of law, it is usually in the form of a civil suit in which a plaintiff has to prove some actual or potential harm. See, e.g., *Presbyterian Church v. United States*, 870 F.2d 518 (9th Cir. 1989) (challenging INS surveillance of churches). In a criminal trial, a defendant may seek either or both of two remedies as part of a claim that his or her First Amendment rights were violated: suppression of evidence gathered in the alleged First Amendment violation, a claim typically analyzed under the “reasonableness” clause of the Fourth Amendment, and dismissal of the indictment on the basis of “outrageous government conduct” in violation of the Due Process Clause of the Fifth Amendment.

(U) The scope of First Amendment rights and their impact on FBI investigative activity are discussed below. The First Amendment’s “establishment clause”—the prohibition against the government establishing or sponsoring a specific religion—has little application to the FBI and, therefore, is not discussed here.

4.2.1 (U) FREE SPEECH

(U) The exercise of free speech includes far more than simply speaking on a controversial topic in the town square. It includes such activities as carrying placards in a parade, sending letters to a newspaper editor, posting information on the Internet, wearing a tee shirt with a political message, placing a bumper sticker critical of the President on one’s car, and publishing books or articles. The common thread in these examples is conveying a public message or an idea through words or deeds. Law enforcement activity that diminishes a person’s ability to communicate in any of these ways may interfere with his or her freedom of speech—and thus may not be undertaken by the FBI solely for that purpose.

(U) It is important to understand the line between constitutionally protected speech and advocacy of violence or of conduct that may lead to violence or other unlawful activity. In *Brandenburg v. Ohio*, 395 U.S. 444 (1969), the Supreme Court established a two-part test to determine whether

such speech is constitutionally protected: the government may not prohibit advocacy of force or violence except when such advocacy (i) is intended to incite imminent lawless action, and (ii) is likely to do so. Therefore, even heated rhetoric or offensive provocation that could conceivably lead to a violent response in the future is usually protected. Suppose, for example, a politically active group advocates on its web site taking unspecified “action” against persons or entities it views as the enemy, who thereafter suffer property damage and/or personal injury. Under the *Brandenburg* two-part test, the missing specificity and imminence in the message may provide it constitutional protection. For that reason, law enforcement may take no action that, in effect, blocks the message or punishes its sponsors.

(U) Despite the high standard for interfering with free speech or punishing those engaged in it, the law does not preclude FBI employees from observing and collecting any of the forms of protected speech and considering its content—as long as those activities are done for a valid law enforcement or national security purpose and are conducted in a manner that does not unduly infringe upon the ability of the speaker to deliver his or her message. To be an authorized purpose it must be one that is authorized by the AGG-Dom—i.e., to further an FBI Assessment, Predicated Investigation, or other authorized function such as providing assistance to other agencies. Furthermore, by following the standards for opening or approving an Assessment or Predicated Investigation as contained in the DIOG, the FBI will ensure that there is a rational relationship between the authorized purpose and the protected speech to be collected such that a reasonable person with knowledge of the circumstances could understand why the information is being collected.

(U) Returning to the example posed above, because the group’s advocacy of action could be directly related by circumstance to property damage suffered by one of the group’s known targets, collecting the speech—although constitutionally protected—can lawfully occur. Similarly, listening to and documenting the public talks by a religious leader, who is suspected of raising funds for a terrorist organization, may yield clues as to his motivation, plan of action, and/or hidden messages to his followers. FBI employees should not, therefore, avoid collecting First Amendment protected speech if it is relevant to an authorized AGG-Dom purpose—as long as FBI employees do so in a manner that does not inhibit the delivery of the message or the ability of the audience to hear it, and so long as the collection is done in accordance with the discussion of least intrusive means or method in Section 4.4.

(U) In summary, during the course of lawful investigative activities, the FBI may lawfully collect, retain, and consider the content of constitutionally protected speech, so long as: (i) the collection is logically related to an authorized investigative purpose; (ii) the collection does not actually infringe on the ability of the speaker to deliver his or her message; and (iii) the method of collection complies with the least intrusive method policy.

4.2.2 (U) EXERCISE OF RELIGION

(U) Like the other First Amendment freedoms, the “free exercise of religion” clause is broader than commonly believed. First, it covers any form of worship of a deity—even forms that are commonly understood to be cults or fringe sects, as well as the right not to worship any deity. Second, protected religious exercise also extends to dress or food that is required by religious edict, attendance at a facility used for religious practice (no matter how unlikely it appears to be intended for that purpose), observance of the Sabbath, raising money for evangelical or

missionary purposes, and proselytizing. Even in controlled environments like prisons, religious exercise must be permitted—subject to reasonable restrictions as to time, place, and manner. Another feature of this First Amendment right is that religion is a matter of heightened sensitivity to some Americans—especially to devout followers. For this reason, religion is a matter that is likely to provoke an adverse reaction if the right is violated—regardless of which religion is involved. Therefore, when essential investigative activity may impact this right, the investigative activity must be conducted in a manner that avoids the actual—and the appearance of—interference with religious practice to the maximum extent possible.

(U) While there must be an authorized purpose for any investigative activity that could have an impact on religious practice, this does not mean religious practitioners or religious facilities are completely free from being examined as part of an Assessment or Predicated Investigation. If such practitioners are involved in—or such facilities are used for—activities that are the proper subject of FBI-authorized investigative or intelligence collection activities, their religious affiliation does not “immunize” them to any degree from these efforts. It is paramount, however, that the authorized purpose of such efforts be properly documented. It is also important that investigative activity directed at religious leaders or at conduct occurring within religious facilities be focused in time and manner so as not to infringe on legitimate religious practice by any individual but especially by those who appear unconnected to the activities under investigation.

(U) Furthermore, FBI employees may take appropriate cognizance of the role religion may play in the membership or motivation of a criminal or terrorism enterprise. If, for example, affiliation with a certain religious institution or a specific religious sect is a known requirement for inclusion in a violent organization that is the subject of an investigation, then whether a person of interest is a member of that institution or sect is a rational and permissible consideration. Similarly, if investigative experience and reliable intelligence reveal that members of a terrorist or criminal organization are known to commonly possess or exhibit a combination of religion-based characteristics or practices (e.g., group leaders state that acts of terrorism are based in religious doctrine), it is rational and lawful to consider such a combination in gathering intelligence about the group—even if any one of these, by itself, would constitute an impermissible consideration. By contrast, solely because prior subjects of an investigation of a particular group were members of a certain religion and they claimed a religious motivation for their acts of crime or terrorism, other members’ mere affiliation with that religion, by itself, is not a basis to assess or investigate—absent a known and direct connection to the threat under Assessment or investigation. Finally, the absence of a particular religious affiliation can be used to eliminate certain individuals from further investigative consideration in those scenarios where religious affiliation is relevant.

4.2.3 (U) FREEDOM OF THE PRESS

(U) Contrary to what many believe, this well-known First Amendment right is not owned by the news media; it is a right of the American people. Therefore, this right covers such matters as reasonable access to news-making events, the making of documentaries, and various other forms of publishing the news. Although the news media typically seek to enforce this right, freedom of the press should not be viewed as a contest between law enforcement or national security, on the one hand, and the interests of news media, on the other. That said, the news gathering function is

the aspect of freedom of the press most likely to intersect with law enforcement and national security investigative activities.

(U) The interest of the news media in protecting confidential sources and the interest of agencies like the FBI in gaining access to those sources who may have evidence of a crime or national security intelligence often clash. The seminal case in this area is *Branzburg v. Hayes*, 408 U.S. 665 (1972), in which the Supreme Court held that freedom of the press does not entitle a news reporter to refuse to divulge the identity of his source to a federal grand jury. The Court reasoned that, as long as the purpose of law enforcement is not harassment or vindictiveness against the press, any harm to the news gathering function of the press (by revealing source identity) is outweighed by the need of the grand jury to gather evidence of crime.

(U) Partially in response to *Branzburg*, the Attorney General promulgated regulations that govern the issuance of subpoenas for reporter's testimony and telephone toll records, the arrest of a reporter for a crime related to news gathering, and the interview of a reporter as a suspect in a crime arising from the news gathering process. In addition, an investigation of a member of the news media in his official capacity, the use of a reporter as a source, and posing as a member of the news media are all sensitive circumstances in the AGG-Dom, DIOG and other applicable AGGs.

(U) These regulations are not intended to insulate reporters and other news media from FBI Assessments or Predicated Investigations. They are intended to ensure that investigative activity that seeks information from or otherwise involves members of the news media:

- A) (U) Is appropriately authorized;
- B) (U) Is necessary for an important law enforcement or national security objective;
- C) (U) Is the least intrusive means to obtain the information or achieve the goals; and
- D) (U) Does not unduly infringe upon the news gathering aspect of the constitutional right to freedom of the press.

4.2.4 (U) FREEDOM OF PEACEFUL ASSEMBLY AND TO PETITION THE GOVERNMENT FOR REDRESS OF GRIEVANCES

(U) Freedom of peaceful assembly, often called the right to freedom of association, presents unique issues for law enforcement agencies, including the FBI. Individuals who gather with others to protest government action, or to rally or demonstrate in favor of, or in opposition to, a social cause sometimes present a threat to public safety by their numbers, by their actions, by the anticipated response to their message, or by creating an opportunity for individuals or other groups with an unlawful purpose to infiltrate and compromise the legitimacy of the group for their own ends. The right to peaceful assembly includes more than just public demonstrations—it includes, as well, the posting of group web sites on the Internet, recruiting others to a cause, marketing a message, and fund raising. All are protected First Amendment activities if they are conducted in support of the organization or political, religious or social cause.

(U) The right to petition the government for redress of grievances is so linked to peaceful assembly and association that it is included in this discussion. A distinction between the two is that an individual may exercise the right to petition the government by himself whereas assembly

necessarily involves others. The right to petition the government includes writing letters to Congress, carrying a placard outside city hall that delivers a political message, recruiting others to one's cause, and lobbying Congress or an executive agency for a particular result.

(U) For the FBI, covert presence or action within associations or organizations, also called “undisclosed participation,” has the greatest potential to impact this constitutional right. The Supreme Court addressed this issue as a result of civil litigation arising from one of the many protests against the Vietnam War. In *Laird v. Tatum*, 408 U.S. 1 (1972), the Court found that the mere existence of an investigative program—consisting of covert physical surveillance in public areas, infiltration of public assemblies by government operatives or sources, and the collection of news articles and other publicly available information—for the purpose of determining the existence and scope of a domestic threat to national security does not, by itself, violate the First Amendment rights of the members of the assemblies. The subjective “chill” to the right to assembly, based on the suspected presence of government operatives, did not by itself give rise to legal “standing” for plaintiffs to argue that their constitutional rights had been abridged. Instead, the Court required a showing that the complained-of government action would reasonably deter the exercise of that right.

(U) Since *Laird v. Tatum* was decided, the lower courts have examined government activity on many occasions to determine whether it gave rise to a “subjective chill” or an “objective deterrent.” The basic standing requirement established by *Laird* remains unchanged today. The lower courts, however, have often imposed a very low threshold of objective harm to survive a motion to dismiss the case. For example, plaintiffs who have shown a loss of membership in an organization, loss of financial support, loss to reputation and status in the community, and loss of employment by members have been granted standing to sue.

(U) More significant for the FBI than the standing issue has been the lower courts’ evaluation of investigative activity into First Amendment protected associations since *Laird*. The courts have held the following investigative activities to be constitutionally permissible under First Amendment analysis:

- A) (U) Undercover participation in group activities;
- B) (U) Physical and video surveillance in public areas;
- C) (U) Properly authorized electronic surveillance;
- D) (U) Recruitment and operation of sources;
- E) (U) Collection of information from government, public, and private sources (with consent); and
- F) (U) The dissemination of information for a valid law enforcement purpose.

(U) However, these decisions were not reached in the abstract. In every case in which the courts have found government action to be proper, the government proved that the action was conducted for an authorized law enforcement or national security purpose and that the action was conducted in substantial compliance with controlling regulations. In addition, in approving these techniques, the courts have often considered whether a less intrusive technique was available to the agency, and the courts have balanced the degree of intrusion or impact against the importance of the law enforcement or national security objective.

(U) By contrast, since *Laird*, the courts have found these techniques to be legally objectionable:

- A) (U) Opening an investigation solely because of the group's social or political agenda (even if the agenda made the group susceptible to subversive infiltration);
- B) (U) Sabotaging or neutralizing the group's legitimate social or political agenda;
- C) (U) Disparaging the group's reputation or standing;
- D) (U) Leading the group into criminal activity that otherwise probably would not have occurred; and
- E) (U) Undermining legitimate recruiting or funding efforts.

(U) In every such case, the court found the government's purpose was not persuasive, was too remote, or was too speculative to justify the intrusion and the potential harm to the exercise of First Amendment rights.

(U) Once again, the message is clear that investigative activity that involves assemblies or associations of individuals in the United States exercising their First Amendment rights must have an authorized purpose under the AGG-Dom—and one to which the information sought and the technique to be employed are rationally related. Less intrusive techniques should always be explored first and those authorizing such activity (which, as discussed above, will almost always constitute a sensitive investigative matter) should ensure that the investigative activity is focused as narrowly as feasible and that the purpose is thoroughly documented.

4.3 (U) EQUAL PROTECTION UNDER THE LAW

4.3.1 (U) INTRODUCTION

(U) The Equal Protection Clause of the United States Constitution provides in part that: "No State shall make or enforce any law which shall deny to any person within its jurisdiction the equal protection of the laws." The Supreme Court and the lower courts have made it clear that the Equal Protection Clause applies to the official acts of United States government law enforcement agents. See, e.g., *Whren v. United States*, 517 U.S. 806 (1996); see also *Chavez v. Illinois State Police*, 251 F.3d 612 (7th Cir. 2001).

Specifically, government employees are prohibited from engaging in invidious discrimination against individuals on the basis of race, ethnicity, national origin, or religious affiliation. This principle is further reflected and implemented for federal law enforcement in the United States Department of Justice's *Guidance Regarding the Use of Race by Federal Law Enforcement Agencies* (hereinafter "DOJ Guidance on the Use of Race").

(U) Investigative and intelligence collection activities must not be based solely on race, ethnicity, national origin, or religious affiliation. Any such activities that are based solely on such considerations are invidious by definition, and therefore, unconstitutional. This standard applies to all investigative and collection activity, including collecting and retaining information, opening investigations, disseminating information, and indicting and prosecuting defendants. It is particularly applicable to the retention and dissemination of personally identifying information about an individual—as further illustrated in the examples enumerated below.

(U) The constitutional prohibition against invidious discrimination based on race, ethnicity, national origin or religion is relevant to both the national security and criminal investigative programs of the FBI. National security investigations often have ethnic aspects; members of a foreign terrorist organization may be primarily or exclusively from a particular country or area of the world. Similarly, ethnic heritage is frequently the common thread running through violent gangs or other criminal organizations. It should be noted that this is neither a new nor isolated phenomenon. Ethnic commonality among criminal and terrorist groups has been relatively constant and widespread across many ethnicities throughout the history of the FBI.

4.3.2 (U) POLICY PRINCIPLES

(U) To ensure that Assessment and investigative activities and strategies consider racial, ethnic, national origin and religious factors properly and effectively and to help assure the American public that the FBI does not engage in invidious discrimination, the DIOG establishes the following policy principles:

- A) (U) The prohibition on basing investigative activity solely on race or ethnicity is not avoided by considering it in combination with other prohibited factors. For example, a person of a certain race engaging in lawful public speech about his religious convictions is not a proper subject of investigative activity based solely on any one of these factors—or by their combination. Before collecting and using information on race, religion or other prohibited factors, a well-founded and authorized investigative purpose must exist beyond these prohibited factors.
- B) (U) When race or ethnicity is a relevant factor to consider, it should not be the dominant or primary factor. Adherence to this standard will not only ensure that it is never the sole factor—it will also preclude undue and unsound reliance on race or ethnicity in investigative analysis. It reflects the recognition that there are thousands and, in some cases, millions of law abiding people in American society of the same race or ethnicity as those who are the subjects of FBI investigative activity, and it guards against the risk of sweeping them into the net of suspicion without a sound investigative basis.
- C) (U) The FBI will not collect or use behavior or characteristics common to a particular racial or ethnic community as investigative factors unless the behavior or characteristics bear clear and specific relevance to a matter under Assessment or investigation. This policy is intended to prevent the potential that collecting ethnic characteristics or behavior will inadvertently lead to individual identification based solely on such matters, as well as to avoid the appearance that the FBI is engaged in ethnic or racial profiling.

4.3.3 (U) GUIDANCE ON THE USE OF RACE AND ETHNIC IDENTITY IN ASSESSMENTS AND PREDICATED INVESTIGATIONS

(U) Considering the reality of common ethnicity or race among many criminal and terrorist groups, some question how the prohibition against racial or ethnic profiling is to be effectively applied—and not violated—in FBI Assessments and Predicated Investigations. The question arises generally in two contexts: (i) with respect to an individual or a group of individuals; and (ii) with respect to ethnic or racial communities as a whole.

4.3.3.1 (U) INDIVIDUAL RACE OR ETHNICITY AS A FACTOR

(U) The DOJ Guidance on the Use of Race permits the consideration of ethnic and racial identity information based on specific reporting—such as from an eyewitness. As a general rule, race or ethnicity as an identifying feature of a suspected perpetrator, subject, and in some cases, a victim, is relevant if it is based on reliable evidence or information—not conjecture or stereotyped assumptions. In addition, the DOJ Guidance on the Use of Race permits consideration of race or ethnicity in other investigative or collection scenarios if it is relevant. These examples illustrate:

- A) (U) The race or ethnicity of suspected members, associates, or supporters of an ethnic-based gang or criminal enterprise may be collected and retained when gathering information about or investigating the organization.
- B) (U) Ethnicity may be considered in evaluating whether a subject is—or is not—a possible associate of a criminal or terrorist group that is known to be comprised of members of the same ethnic grouping—as long as it is not the dominant factor for focusing on a particular person. It is axiomatic that there are many members of the same ethnic group who are not members of the criminal or terrorist group; for that reason, there must be other information beyond race or ethnicity that links the individual to the terrorist or criminal group or to the other members of the group. Otherwise, racial or ethnic identity would be the sole criterion, and that is impermissible.

4.3.3.2 (U) COMMUNITY RACE OR ETHNICITY AS A FACTOR

4.3.3.2.1 (U) COLLECTING AND ANALYZING DEMOGRAPHICS

(U) The DOJ Guidance on the Use of Race and FBI policy permit the FBI to identify locations of concentrated ethnic communities in the field office's domain, if these locations will reasonably aid the analysis of potential threats and vulnerabilities, and, overall, assist domain awareness for the purpose of performing intelligence analysis. If, for example, intelligence reporting reveals that members of certain terrorist organizations live and operate primarily within a certain concentrated community of the same ethnicity, the location of that community is clearly valuable—and properly collectible—data. Similarly, the locations of ethnic-oriented businesses and other facilities may be collected if their locations will reasonably contribute to an awareness of threats and vulnerabilities, and intelligence collection opportunities. Also, members of some communities may be potential victims of civil rights crimes and, for this reason, community location may aid enforcement of civil rights laws. Information about such communities should not be collected, however, unless the communities are sufficiently concentrated and established so as to provide a reasonable potential for intelligence collection that would support FBI mission programs (e.g., where identified terrorist subjects from certain countries may relocate to blend in and avoid detection).

4.3.3.2.2 (U) GEO-MAPPING ETHNIC/RACIAL DEMOGRAPHICS

(U) As a general rule, if information about community demographics may be collected, it may be “mapped.” Sophisticated computer geo-mapping technology visually depicts lawfully collected information and can assist in showing relationships among disparate data. By itself,

mapping raises no separate concerns about racial or ethnic profiling, assuming the underlying information that is mapped was properly collected. It may be used broadly - e.g., for domain awareness of all relevant demographics in the field office's area of responsibility or to track crime trends - or narrowly to identify specific communities or areas of interest to inform a specific Assessment or investigation. In each case, the relevance of the ethnic or racial information mapped to the authorized purpose of the Assessment or investigation must be clearly demonstrated and documented.

4.3.3.2.3 (U) GENERAL ETHNIC/RACIAL BEHAVIOR

(U) The authority to collect ethnic community location information does not extend to the collection of cultural and behavioral information about an ethnic community that bears no rational relationship to a valid investigative or analytical need. Every ethnic community in the Nation that has been associated with a criminal or national security threat has a dominant majority of law-abiding citizens, resident aliens, and visitors who may share common ethnic behavior but who have no connection to crime or terrorism (as either subjects or victims). For this reason, a broad-brush collection of racial or ethnic characteristics or behavior is not helpful to achieve any authorized FBI purpose and may create the appearance of improper racial or ethnic profiling.

4.3.3.2.4 (U) SPECIFIC AND RELEVANT ETHNIC BEHAVIOR

(U) On the other hand, knowing the behavioral and life style characteristics of known individuals who are criminals or who pose a threat to national security may logically aid in the detection and prevention of crime and threats to the national security within the community and beyond. Focused behavioral characteristics reasonably believed to be associated with a particular criminal or terrorist element of an ethnic community (not with the community as a whole) may be collected and retained. For example, if it is known through intelligence analysis or otherwise that individuals associated with an ethnic-based terrorist or criminal group conduct their finances by certain methods, travel in a certain manner, work in certain jobs, or come from a certain part of their home country that has established links to terrorism, those are relevant factors to consider when investigating the group or assessing whether it may have a presence within a community. It is recognized that the "fit" between specific behavioral characteristics and a terrorist or criminal group is unlikely to be perfect—that is, there will be members of the group who do not exhibit the behavioral criteria as well as persons who exhibit the behaviors who are not members of the group. Nevertheless, in order to maximize FBI mission relevance and to minimize the appearance of racial or ethnic profiling, the criteria used to identify members of the group within the larger ethnic community to which they belong must be as focused and as narrow as intelligence reporting and other circumstances permit. If intelligence reporting is insufficiently exact so that it is reasonable to believe that the criteria will include an unreasonable number of people who are not involved, then it would be inappropriate to use the behaviors, standing alone, as the basis for FBI activity.

4.3.3.2.5 (U) EXPLOITIVE ETHNIC BEHAVIOR

(U) A related category of information that can be collected is behavioral and cultural information about ethnic or racial communities that is reasonably likely to be exploited by criminal or terrorist groups who hide within those communities in order to engage in illicit activities undetected. For example, the existence of a cultural tradition of collecting funds from members within the community to fund charitable causes in their homeland at a certain time of the year (and how that is accomplished) would be relevant if intelligence reporting revealed that, unknown to many donors, the charitable causes were fronts for terrorist organizations or that terrorist supporters within the community intended to exploit the unwitting donors for their own purposes.

4.4 (U) LEAST INTRUSIVE METHOD

4.4.1 (U) OVERVIEW

(U) The AGG-Dom requires that the "least intrusive" means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of a more intrusive method. This principle is also reflected in See Appendix B: Executive Order 12333, which governs the activities of the United States Intelligence Community. The concept of least intrusive method applies to the collection of all information. Regarding the collection of foreign intelligence that is not collected as part of the FBI's traditional national security or criminal missions, the AGG-Dom further requires that open and overt collection activity must be used with USPERs, if feasible.

(U) By emphasizing the use of the least intrusive means to obtain information, FBI employees can effectively execute their duties while mitigating potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary information, but rather is intended to encourage investigators to choose the least intrusive—but still reasonable—means from the available options to obtain the information.

(U) This principle is embodied in statutes and DOJ policies on a variety of topics including electronic surveillance, the use of tracking devices, the temporary detention of suspects, and forfeiture. In addition, the concept of least intrusive method can be found in case law as a factor to be considered in assessing the reasonableness of an investigative method in the face of a First Amendment or due process violation claim. See *Clark v. Library of Congress*, 750 F.2d 89, 94-5 (D.C. Cir. 1984); *Alliance to End Repression v. City of Chicago*, 627 F. Supp. 1044, 1055 (N.D. Ill. 1985), citing *Elrod v. Burns*, 427 U.S. 347, 362-3 (1976).

4.4.2 (U) GENERAL APPROACH TO LEAST INTRUSIVE METHOD CONCEPT

(U) Determining what constitutes the least intrusive method in an investigative or intelligence collection scenario is both a logical process and an exercise in judgment. It is logical in the sense that the FBI employee must first confirm that the selected technique will:

- A) (U) Gather information that is relevant to the Assessment or Predicated Investigation;

- B) (U) Acquire the information within the time frame required by the assessment or Predicated Investigation;
- C) (U) Gather the information consistent with operational security and the protection of sensitive sources and methods; and
- D) (U) Gather information in a manner that provides confidence in its accuracy.

(U) Determining the least intrusive method also requires sound judgment because the factors discussed above are not fixed points on a checklist. They require careful consideration based on a thorough understanding of investigative objectives and circumstances.

4.4.3 (U) DETERMINING INTRUSIVENESS

(U) The degree of procedural protection that established law and the AGG-Dom provide for the use of the method helps to determine its intrusiveness. Using this factor, search warrants, wiretaps, and undercover operations are very intrusive. By contrast, investigative methods with limited procedural requirements, such as checks of government and commercial data bases and communication with established sources, are less intrusive.

(U) The following guidance is designed to assist FBI personnel in judging the relative intrusiveness of different methods:

- A) (U) **Nature of the information sought:** Investigative objectives generally dictate the type of information required and from whom it should be collected. This subpart is not intended to address the situation where the type of information needed and its location are so clear that consideration of alternatives would be pointless. When the option exists to seek information from any of a variety of places, however, it is less intrusive to seek information from less sensitive and less protected places. Similarly, obtaining information that is protected by a statutory scheme (e.g., financial records) or an evidentiary privilege (e.g., attorney/client communications) is more intrusive than obtaining information that is not so protected. In addition, if there exists a reasonable expectation of privacy under the Fourth Amendment (i.e., private communications), obtaining that information is more intrusive than obtaining information that is knowingly exposed to public view as to which there is no reasonable expectation of privacy.
- B) (U) **Scope of the information sought:** Collecting information regarding an isolated event—such as a certain phone number called on a specific date or a single financial transaction—is less intrusive or invasive of an individual's privacy than collecting a complete communications or financial "profile." Similarly, a complete credit history is a more intrusive view into an individual's life than a few isolated credit charges. In some cases, of course, a complete financial and credit profile is exactly what the investigation requires (for example, investigations of terrorist financing or money laundering). If so, FBI employees should not hesitate to use appropriate legal process to obtain such information if the predicate requirements are satisfied. Operational security—such as source protection—may also dictate seeking a wider scope of information than is absolutely necessary for the purpose of protecting a specific target or source. When doing so, however, the concept of least intrusive method still applies. The FBI may obtain more data than strictly needed, but it should obtain no more data than is needed to accomplish the investigative or operational security purpose.
- C) (U) **Scope of the use of the method:** Using a method in a manner that captures a greater picture of an individual's or a group's activities are more intrusive than using the same method or a different one that is focused in time and location to a specific objective. For example, it is

less intrusive to use a tracking device to verify point-to-point travel than it is to use the same device to track an individual's movements over a sustained period of time. Sustained tracking on public highways would be just as lawful but more intrusive because it captures a greater portion of an individual's daily movements. Similarly, surveillance by closed circuit television that checks a discrete location within a discrete time frame is less intrusive than 24/7 coverage of a wider area. For another example, a computer intrusion device that captures only host computer identification information is far less intrusive than one that captures file content.

- D) (U) *Source of the information sought:* It is less intrusive to obtain information from existing government sources (such as state, local, tribal, international, or federal partners) or from publicly-available data in commercial data bases, than to obtain the same information from a third party (usually through legal process) that has a confidential relationship with the subject—such as a financial or academic institution. Similarly, obtaining information from a reliable confidential source who is lawfully in possession of the information and lawfully entitled to disclose it (such as obtaining an address from an employee of a local utility company) is less intrusive than obtaining the information from an entity with a confidential relationship with the subject. It is recognized in this category that the accuracy and procedural reliability of the information sought is an important factor in choosing the source of the information. For example, even if the information is available from a confidential source, a grand jury subpoena, national security letter, ex parte order, or other process may be required in order to ensure informational integrity and accuracy.
- E) (U) *The risk of public exposure:* Seeking information about an individual or group under circumstances that create a risk that the contact itself and the information sought will be exposed to the individual's or group's detriment and/or embarrassment—particularly if the method used carries no legal obligation to maintain silence—is more intrusive than information gathering that does not carry that risk. Interviews with employers, neighbors, and associates, for example, or the issuance of grand jury subpoenas at a time when the investigation has not yet been publicly exposed are more intrusive than methods that gather information covertly. Similarly, interviews of a subject in a discrete location would be less intrusive than an interview at, for example, a place of employment or other location where the subject is known.

(U) There is a limit to the utility of this list of intrusiveness factors. Some factors may be inapplicable in a given investigation and, in many cases, the choice and scope of the method will be dictated wholly by investigative objectives and circumstances. The foregoing is not intended to provide a comprehensive checklist or even an overall continuum of intrusiveness. It is intended instead to identify the factors involved in a determination of intrusiveness and to attune FBI employees to select, within each applicable category, a less intrusive method if operational circumstances permit. In the end, selecting the least intrusive method that will accomplish the objective is a matter of sound judgment. In exercising such judgment, however, consideration of these factors should ensure that the decision to proceed is well founded.

4.4.4 (U) STANDARD FOR BALANCING INTRUSION AND INVESTIGATIVE REQUIREMENTS

(U) Once an appropriate method and its deployment have been determined, reviewing and approving authorities should balance the level of intrusion against investigative requirements. This balancing test is particularly important when the information sought involves clearly established constitutional, statutory, or evidentiary rights or sensitive circumstances (such as obtaining information from religious or academic institutions or public fora where First

Amendment rights are being exercised), but should be applied in all circumstances to ensure that the least intrusive method if reasonable based upon the circumstances of the investigation is being utilized.

(U) Balancing the factors discussed above with the considerations discussed below will help determine whether the method and the extent to which it intrudes into privacy or threatens civil liberties are proportionate to the significance of the case and the information sought.

(U) Considerations on the investigative side of the balancing scale include the:

- A) (U) Seriousness of the crime or national security threat;
- B) (U) Strength and significance of the intelligence/information to be gained;
- C) (U) Amount of information already known about the subject or group under investigation; and
- D) (U) Requirements of operational security, including protection of sources and methods.

(U) If, for example, the threat is remote, the individual's involvement is speculative, and the probability of obtaining probative information is low, intrusive methods may not be justified, and, in fact, they may do more harm than good. At the other end of the scale, if the threat is significant and possibly imminent (e.g., a bomb threat), aggressive measures would be appropriate regardless of intrusiveness.

(U) In addition, with respect to the investigation of a group, if the terrorist or criminal nature of the group and its membership is well established (e.g., al Qaeda, Ku Klux Klan, Colombo Family of La Cosa Nostra), there is less concern that pure First Amendment activity is at stake than there would be for a group whose true character is not yet known (e.g., an Islamic charity suspected of terrorist funding) or many of whose members appear to be solely exercising First Amendment rights (anti-war protestors suspected of being infiltrated by violent anarchists). This is not to suggest that investigators should be less aggressive in determining the true nature of an unknown group that may be engaged in terrorism or other violent crime. Indeed, a more aggressive and timely approach may be in order to determine whether the group is violent or to eliminate it as a threat. Nevertheless, when First Amendment rights are at stake, the choice and use of investigative methods should be focused in a manner that minimizes potential infringement of those rights. Finally, as the investigation progresses and the subject's or group's involvement becomes clear, more intrusive methods may be justified. Conversely, if reliable information emerges refuting the individual's involvement or the group's criminal or terrorism connections, the use of any investigative methods must be carefully reconsidered.

(U) Another consideration to be balanced is operational security: if a less intrusive but reasonable method were selected, would the subject detect its use and alter his activities—including his means of communication—to thwart the success of the operation? Operational security—particularly in national security investigations—should not be undervalued and may, by itself, justify covert tactics which, under other circumstances, would not be the least intrusive.

4.4.5 (U) CONCLUSION

(U) The foregoing guidance is offered to assist FBI employees in navigating the often unclear course to select the least intrusive investigative method that effectively accomplishes the operational objective at hand. In the final analysis, choosing the method that must appropriately

balances the impact on privacy and civil liberties with operational needs, is a matter of judgment, based on training and experience. Pursuant to the AGG-Dom, other applicable laws and policies, and this guidance, FBI employees may use any lawful method allowed, even if intrusive, where the intrusiveness is warranted by the threat to the national security or to potential victims of crime and/or the strength of the information indicating the existence of that threat.

5 (U) ASSESSMENTS

5.1 (U) OVERVIEW AND ACTIVITIES AUTHORIZED PRIOR TO OPENING AN ASSESSMENT

(U//FOUO) The AGG-Dom combines “threat assessments” under the former *Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* and the “prompt and extremely limited checking out of initial leads” under the former *Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* into a new investigative category entitled “Assessments.”

(U//FOUO) All Assessments must be documented in the appropriate form, to include an FD-71, Guardian (FD-71a), or EC, and the form must be placed in one of the following files:

- A) (U//FOUO) investigative classification as an Assessment file (e.g., 415A-WF-xxxxxx);
- B) (U//FOUO) zero sub-assessment file (e.g., 91-0-ASSESS-D; 15-0-ASSESS; 315-0-ASSESS-D);
- C) (U//FOUO) zero classification file (e.g. 196-WF-0). This file may be used if information is entered in the FD-71 or FD-71a and an Assessment is not opened based on that information;
- D) (U//FOUO) 800 series (801-807) classification file, as discussed in greater detail below;
- E) (U//FOUO) unaddressed work file; or
- F) (U//FOUO) existing open or closed file.

(U//FOUO) Note: In the DIOG, the word “assessment” has two distinct meanings. The AGG-Dom authorizes as an investigative activity an “Assessment,” which requires an authorized purpose as discussed in this section of the DIOG. The USIC, however, also uses the word “assessment” to describe written intelligence products, as discussed in DIOG Sections 15.2.3 and 15.6.1.2.

(U) Assessments authorized under the AGG-Dom do not require a particular factual predication but do require an authorized purpose and clearly defined objective(s). Assessments may be carried out to detect, obtain information about, or prevent or protect against Federal crimes or threats to the national security or to collect foreign intelligence. (AGG-Dom, Part II and Part II.A)

(U//FOUO) Although “no particular factual predication” is required, the basis of an Assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject. Although difficult to define, “no particular factual predication” is less than “information or allegation” as required for the initiation of a preliminary investigation (PI). For example, an Assessment may be conducted when: (i) there is reason to collect information or facts to determine whether there is a criminal or national security threat; and (ii) there is a rational and articulable relationship between the stated authorized purpose of the Assessment on the one hand and the information sought and the proposed means to obtain that information on the other. An FBI employee must be able to explain the authorized purpose and the clearly

defined objective(s), and reason the particular investigative methods were used to conduct the Assessment. FBI employees who conduct Assessments are responsible for ensuring that Assessments are not pursued for frivolous or improper purposes and are not based solely on First Amendment activity or on the race, ethnicity, national origin, or religion of the subject of the Assessment, or a combination of only such factors. (AGG-Dom, Part II)

(U//FOUO) When employees undertake activities authorized in DIOG Section 5.1.1 below prior to opening an Assessment they must have a reason to undertake these activities that is tied to an authorized FBI criminal or national security purpose.

5.1.1 (U) ACTIVITIES AUTHORIZED PRIOR TO OPENING AN ASSESSMENT

(U//FOUO) When initially processing a complaint, observation, or information, an FBI employee can use the following investigative methods:

5.1.1.1 (U) PUBLIC INFORMATION

(U//FOUO) See DIOG section 18.5.1.

(U//FOUO) Prior to opening an Assessment, consent searches are not authorized. However, if in the course of processing a complaint or conducting a clarifying interview of the complainant, the complainant volunteers to provide access to his personal or real property, an agent may accept and conduct a search of the item(s) or property voluntarily provided.

5.1.1.2 (U) RECORDS OR INFORMATION - FBI AND DOJ

(U//FOUO) See DIOG section 18.5.2.

5.1.1.3 (U) RECORDS OR INFORMATION – OTHER FEDERAL, STATE, LOCAL, TRIBAL, OR FOREIGN GOVERNMENT AGENCY

(U//FOUO) See DIOG Section 18.5.3.

5.1.1.4 (U) ON-LINE SERVICES AND RESOURCES

(U//FOUO) See DIOG Section 18.5.4.

5.1.1.5 (U) CLARIFYING INTERVIEW

(U//FOUO) Conduct a voluntary clarifying interview of the complainant or the person who initially furnished the information.

(U//FOUO) See DIOG Section 18.5.6.

5.1.1.6 (U) INFORMATION VOLUNTARILY PROVIDED BY GOVERNMENTAL OR PRIVATE ENTITIES

(U//FOUO) See DIOG Section 18.5.7.

(U//FOUO) With the benefit of a clarifying interview, checking records (existing/historical information), and/or asking an existing CHS about something that he or she already knows, an

FBI employee may be able to answer the following question when evaluating the initial complaint, observation, or information: Does the complaint, observation, or information appear to represent a credible basis to open an Assessment, with an authorized purpose and clearly defined objective(s), or to open a Predicated Investigation consistent with the standards set forth in the DIOG?

(U//FOUO) **Intelligence Analysis and Planning:** These activities may allow the FBI employee to resolve a matter without the need to conduct new investigative activity, for which an Assessment or a Predicated Investigation must be opened. When conducting clarifying interviews and checking records as described above, FBI employees must always adhere to the core values and principles articulated in DIOG Sections 3 and 4.

5.1.2 (U) DOCUMENTATION REQUIREMENTS FOR RECORD CHECKS: (EXISTING /HISTORICAL INFORMATION REFERRED TO IN SECTION 5.1.1 ABOVE)

(U//FOUO) FBI employees must document and retain records checks in an FD-71, FD-71a or successor intake form or other system of records if, in the judgment of the FBI employee, there is a law enforcement, intelligence or public safety purpose to do so. If such record checks are documented, they must also be retained in one of the following files:

- A) (U//FOUO) zero classification file when no further investigative activity is warranted;
- B) (U//FOUO) relevant open or closed zero sub-assessment file;
- C) (U//FOUO) relevant open or closed Predicated Investigation file;
- D) (U//FOUO) new Assessment or Predicated Investigation file, when further investigative activity is warranted; or
- E) (U//FOUO) unaddressed work file.

(U//FOUO) Additionally, through analysis of existing information, the FBI employee may produce products that include, but are not limited to: an Intelligence Assessment, Intelligence Bulletin and Geospatial Intelligence (mapping). If, while conducting analysis, the FBI employee finds a gap in intelligence that is relevant to an authorized FBI activity, then the FBI employee can identify the gap for possible development of a "collection requirement." The FBI employee must document this analysis in the applicable 801-807 classification file (or other 800-series classification file as directed in the Intelligence Policy Implementation Guide (IPG)). See the IPG for file classification guidance.

5.1.3 (U) LIAISON ACTIVITIES AND TRIPWIRES

(U) Some FBI activities are not traditional investigative or intelligence activities. Activities such as liaison, tripwires, and other community outreach represent relationship-building efforts or other pre-cursors to developing and maintaining good partnerships. These activities are critical to the success of the FBI's mission. DIOG Section 11 addresses liaison activities and tripwires.

5.2 (U) PURPOSE AND SCOPE

(U//FOUO) The FBI cannot be content to wait for leads to come in through the actions of others; rather, we must be vigilant in detecting criminal or national security threats to the full extent

permitted by law, with an eye towards early intervention and prevention of criminal or national security incidents before they occur. For example, to carry out the central mission of protecting the national security, the FBI must proactively collect information from available sources in order to identify threats and activities and to inform appropriate intelligence analysis. Collection required to inform such analysis will appear as FBI National Collection Requirements and FBI Field Office Collection Requirements. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity or facility has drawn the attention of would-be perpetrators of crime or terrorism. The proactive authority conveyed to the FBI is designed for, and may be used by, the FBI in the discharge of these responsibilities. The FBI may also conduct Assessments as part of its special events management responsibilities. (AGG-Dom, Part II)

(U) More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots to come to fruition. Hence, Assessments may also be undertaken proactively with such purposes as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization in such activities; and identifying and assessing individuals who may have value as confidential human sources. (AGG-Dom, Part II).

(U//FOUO) As described in the scenarios below, Assessments may be used when an “allegation or information” or an “articulable factual basis” (the predicates for Predicated Investigations) concerning crimes or threats to the national security is obtained and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in Assessments (use of least intrusive means). The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity (Predicated Investigation), if the results of an Assessment indicate that further investigation is not warranted. (AGG-Dom, Part II)
Hypothetical fact patterns are discussed below:

5.2.1 (U) SCENARIOS

(U//FOUO) **Scenario 1:** Based upon a newspaper or trusted publication article related to an emerging criminal problem, an FBI employee wishes to analyze information/data already contained in FBI data systems, query ChoicePoint, NCIC and search the Internet for information to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone.

(U//FOUO) **Response 1:** The FBI employee can query and analyze record checks in computer database systems, including the Internet, without opening an Assessment pursuant to Section 5.1.1.1-5. The FBI employee may produce products that include, but are not limited to, Intelligence Assessments, Intelligence Bulletin and Geospatial Intelligence (mapping). Additionally, if the FBI employee identifies a gap in intelligence relevant to an authorized FBI activity, the FBI employee may submit the gap for possible development as a “collection requirement.” As specified in Section 5.1.2 above, the FBI employee may document this analysis in the applicable 801-807 classification file (or

other 800-series classification file as directed in the IPG). See the IPG for file classification guidance.

(U//FOUO) Because the FBI employee has not conducted any new investigative activity or used an investigative method described in DIOG Sections 18.5 – 18.7 these queries can be made without opening an Assessment.

(U//FOUO) **Scenario 2:** A marina owner contacts the local FBI office stating that five Middle Eastern males have just rented a boat for three days and asked for marine charts.

(U//FOUO) **Response 2:** Without additional information, it would not be appropriate to conduct an Assessment, because there is no indication of criminal conduct, a threat to the national security, or information that might be foreign intelligence information. The fact that the men are Middle Eastern is not, standing alone, a reason to open an Assessment.

(U//FOUO) **Scenario 3:** A marina owner contacts the local FBI office stating that five males, who appear to be Middle Eastern, have just rented a boat for three days and asked for marine charts. The owner also stated the men asked him to circle the military installations and nuclear power plants on the marine charts.

(U//FOUO) **Response 3:** Because of the potential for either criminal activity or a threat to the national security, this scenario provides an authorized purpose for conducting an Assessment. The FBI can conduct an Assessment for the purpose of ascertaining the intentions of the five males. In this scenario, the men's national origin is not the motivating factor for the Assessment. It could, however, be a factor the FBI would consider in conducting the Assessment if relevant intelligence makes their national origin relevant (for example, if existing intelligence reporting suggested that Al Qaeda was planning an attack using boats as a means of attack).

(U//FOUO) **Scenario 4:** A field office wishes to acquire the following information/data within its Area of Responsibility (AOR) in order to proactively identify threats and domain awareness, including: (i) general demographics (e.g., general population to include concentrations of racial and ethnic groups; location of religious institutions); (ii) location of violent gang activity; (iii) residences of parolees and probationers; and (iv) location of military installations and defense contractors. After acquiring this information/data, the field office wants to map it.

(U//FOUO) **Response 4:** A Type 4 Assessment with an authorized purpose for gathering this data must be opened so that a field office can acquire all of the above information. In this scenario, the authorized purpose would be to facilitate intelligence analysis and planning. In addition to an "authorized purpose," a field office must also have a clearly defined objective(s) for acquiring the particular information and data, which may not be based solely on activities protected by the First Amendment or on race, ethnicity, national origin or religion. The FBI employee must document this AOR analysis in the applicable 818A through F or 815 H classification file (or other 800-series classification file as directed in the IPG). See the IPG for file classification guidance.

(U//FOUO) Scenario 4 may only be opened as an Assessment.

(U//FOUO) Scenario 5: While en-route to work in the morning an FBI employee notices two individuals in a parked car in the parking lot of a closed bank. The bank is not scheduled to open for several hours. There is nothing peculiar about the situation other than the fact that the individuals appear to just be sitting there. The bus arrives and the FBI employee goes to work. The next day the FBI employee notices the same two individuals in the same car just sitting in the lot.

(U//FOUO) Response 5: It is unusual for people to sit in a vacant parking lot hours before a business is scheduled to open. The individuals might simply be meeting there to carpool to work, or they may be conducting preoperational surveillance of the bank and surrounding area. The facts as noted do not create the inference or allegation of criminal activity sufficient to open a Preliminary Investigation. In this situation, however, the FBI employee can conduct an Assessment to determine whether the individuals' presence is lawful or not.

(U//FOUO) Scenario 5 may only be opened as an Assessment.

(U//FOUO) Scenario 6: An FBI employee receives a complaint from an individual regarding a letter that was faxed to him from an alleged foreign prince. The letter involved the recovery of a large sum of money if the individual will provide his bank account information to the prince by a telephone number provided in the letter. The letter states the individual should not tell law enforcement about the possible recovery because the money was embezzled from the foreign government.

(U//FOUO) Response 6: Because this is likely a fraud, the FBI can conduct an Assessment for the purpose of determining the validity of the complaint, identifying the subject, the contents of the letter, and to determine whether further investigative action is appropriate. This scenario also meets the standard to open a Preliminary Investigation.

(U//FOUO) Scenario 7: The FBI receives an anonymous letter threatening a "dirty bomb" attack; however, the letter contains inaccurate information about the process for making a "dirty bomb."

(U//FOUO) Response 7: Because of the potential for criminal conduct and a threat to the national security, this scenario provides an authorized purpose for an Assessment. The FBI can conduct an Assessment for the purpose of identifying the drafter of the threatening letter and potential targets or vulnerabilities to criminal activities or threats to the national security. This scenario also meets the standard to open a Preliminary Investigation.

(U//FOUO) Scenario 8: An FBI employee in an FBI field office receives a memorandum from a flight school indicating that it has received a large number of students registering for flight school to learn to fly large commercial airplanes who seem unusually ill-prepared with minimal relevant aviation skills.

(U//FOUO) Response 8: Because of the potential for criminal conduct and a threat to the national security, this scenario provides an authorized purpose for an Assessment. This scenario also meets the standard to open a Preliminary Investigation.

5.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to ensure civil liberties are not infringed upon through Assessments, every Assessment must have an authorized purpose and clearly defined objective(s). The authorized purpose and clearly defined objective(s) of the Assessment must be documented and retained as described in this section and in DIOG Section 14.

(U) Even when an authorized purpose is present, an Assessment could create the appearance that it is directed at or activated by constitutionally-protected activity, race, ethnicity, national origin or religion—particularly under circumstances where the link to an authorized FBI mission is not readily apparent. In these situations, it is vitally important that the authorized purpose and the clearly defined objective(s), as well as the use of any investigative methods, are well documented.

(U) No investigative activity, including Assessments, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only such factors. If an Assessment touches on or is partially motivated by First Amendment activities, or by race, ethnicity, national origin or religion, or a combination of only such factors, it is particularly important to identify and document the basis for the Assessment with clarity.

(U//FOUO) *Example:* Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or advocating a change in government through non-criminal means, and actively recruiting others to join their causes—have a fundamental constitutional right to do so. An Assessment may not be opened based solely on the exercise of these First Amendment rights. If, however, a group exercising its First Amendment rights also threatens or advocates violence or destruction of property, an Assessment would be appropriate.

(U) The AGG-Dom require that the "least intrusive" means or method be considered and—if reasonable based upon the circumstances of the investigation—used in lieu of more intrusive methods to obtain information, intelligence and/or evidence. This principle is also reflected in Executive Order 12333 (see Appendix B), which governs the activities of the USIC. Executive Order 12333 lays out the goals, directions, duties and responsibilities of the USIC. The concept of least intrusive means applies to the collection of all information, intelligence and evidence, not just that collected by those aspects of the FBI that are part of the intelligence community.

(U) By emphasizing the use of the least intrusive means to obtain information, intelligence, and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties and the damage to the reputation of all people encompassed within the investigation or Assessment, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the

investigation—means from the available options to obtain the information. (AGG-Dom, Part I.C.2)

5.4 (U) FIVE TYPES OF ASSESSMENTS (AGG-DOM, PART II.A.3.)

5.4.1 (U) ASSESSMENT TYPES

(U) There are five (5) authorized types of Assessments that may be carried out for the purposes of detecting, obtaining information about, or preventing or protecting against Federal crimes or threats to the national security or to collect foreign intelligence. The types of Assessments are:

- A) (U) Type 1 & 2 Assessment⁴: Seek information, proactively or in response to investigative leads, relating to activities – or the involvement or role of individuals, groups, or organizations relating to those activities – constituting violations of Federal criminal law or threats to the national security;
- B) (U) Type 3 Assessment: Identify, obtain and utilize information about actual or potential national security threats or Federal criminal activities, or the vulnerability to such threats or activities;
- C) (U) Type 4 Assessment: Obtain and retain information to inform or facilitate intelligence analysis and planning;
- D) (U) Type 5 Assessment: Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources; and
- E) (U) Type 6 Assessment: Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.

5.5 (U) STANDARDS FOR OPENING OR APPROVING AN ASSESSMENT

(U//FOUO) Before opening or approving an Assessment, an FBI employee or approving official must determine whether:

- A) (U//FOUO) An authorized purpose and clearly defined objective(s) exists for the conduct of the Assessment;
- B) (U//FOUO) The Assessment is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject, or a combination of only such factors; and
- C) (U//FOUO) The Assessment is an appropriate use of personnel and financial resources.

⁴ (U//FOUO) In the original DIOG (12/16/2008), types 1 and 2 were considered to be separate Assessment types. Because they, however, have many commonalities, they were merged into one type (named a "Type 1 & 2 Assessment") for purposes of this version of the DIOG. Hence, there are now five, not six, types of Assessments.

5.6 (U) POSITION EQUIVALENTS, EFFECTIVE DATE, DURATION, DOCUMENTATION, APPROVAL, NOTICE, FILE REVIEW AND RESPONSIBLE ENTITY

5.6.1 (U) FIELD OFFICE AND FBIHQ POSITION EQUIVALENTS

(U//FOUO) FBIHQ and FBI field offices have the authority to conduct all Assessment activities as authorized in Section 5.4 above. Position equivalents for field office and FBIHQ personnel when FBIHQ opens, conducts, or closes an Assessment are specified in DIOG Section 3.11.

5.6.2 (U) EFFECTIVE DATE OF ASSESSMENTS

(U//FOUO) For all Assessments, the effective date of the Assessment is the date the final approval authority approves the FD-71, Guardian (FD-71a) or EC. Documenting the effective date of an Assessment is important for many reasons, including establishing time frames for justification and file reviews, and extensions. The effective date of the final approval authority occurs when:

- A) (U//FOUO) **For Type 1 & 2 Assessments:** the SSA or SIA opens and assigns the FD-71 or Guardian (FD-71a) to the employee;
(U//FOUO) Note: In Type 1 & 2 Assessments only, employees do not need to obtain supervisory approval prior to opening the Assessment. If, however, oral approval is obtained, employees must memorialize the oral approval date in the body of the FD-71 or Guardian (FD-71a).
- B) (U//FOUO) **For Type 3 – 6 Assessments:** the SSA, SIA, or the DI opens and assigns the Assessment by: (i) the electronic signature/date generated by Sentinel – or successor case management system; or (ii) handwriting his/her initials and date on the EC; or
- C) (U//FOUO) **For Sensitive Investigative Matters (SIM) Assessments:** the SAC (or SC) authorizes the Assessment to be opened and assigned to an FBI employee by: (i) approving the FD-71 or Guardian (FD-71a); (ii) the electronic signature/date generated by Sentinel – or successor case management system; or (iii) handwriting his/her initials and date on the EC. (See DIOG Sections 5.7 and 10).

5.6.3 (U) ASSESSMENT TYPES

(U//FOUO) The applicable duration, documentation, approval level, notice, justification/file review, and responsible entity requirements for each of the five (5) types of Assessments are discussed below.

(U//FOUO) In all types of Assessments, investigative leads, either Action Required or Information Only, may only be set by EC, FD-71 or Guardian (FD-71a).

5.6.3.1 (U) TYPE 1 & 2 ASSESSMENTS

(U) Type 1 & 2 Assessment defined: Seek information, proactively or in response to investigative leads, relating to activities – or the involvement or role of individuals, groups, or organizations in those activities – constituting violations of Federal criminal law or threats to the national security (i.e., the prompt checking of leads on individuals, activity, groups or organizations).

(U//FOUO) See Section 5.11 below for intelligence collection (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the 815I field office file.

5.6.3.1.1 (U) DURATION

(U//FOUO) There is no time limit for a Type 1 & 2 Assessment, but it is anticipated that such Assessments will be relatively short.

5.6.3.1.2 (U) DOCUMENTATION

(U//FOUO) The authorized purpose(s) and clearly defined objective(s) for the Type 1 & 2 Assessment must be documented in the FD-71 or Guardian. Guardian (FD-71a) must be used to document Type 1 & 2 Assessments that pertain to international terrorism, domestic terrorism, weapons of mass destruction terrorism, and cyber terrorism. The electronic FD-71, as discussed below, must be used to document all other Type 1 & 2 Assessments (i.e., criminal, other cyber).

(U//FOUO) An FBI employee must also document in the FD-71 or Guardian (FD-71a) the use of, or the request and approval for the use of, authorized investigative methods. By exception, an EC may be required to document the use and approval of particular investigative methods. The results of the use of investigative methods must also be documented in the FD-71 or Guardian, or by exception, in an EC. The completed FD-71 or Guardian requires supervisor approval before being uploaded.

(U//FOUO) All investigative documents (FD-302's, ECs, surveillance logs, etc.) must be referenced, and attached or linked electronically to the appropriate FD-71 or Guardian consistent with the instructions in the FD-71 and Guardian programs.

(U//FOUO) Type 1 & 2 Assessments that are not converted to a Predicated Investigation must be uploaded to a "zero" sub-assessment file (e.g., 91-0-ASSESS-D, 15-0-ASSESS) within the appropriate classification as described in Section 5.14. The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

5.6.3.1.3 (U) APPROVAL TO OPEN

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment without supervisor approval. After receipt of the complaint or other information that triggers the Assessment, the FBI employee must complete an FD-71 or Guardian as soon as practicable to document this type of Assessment. The SSA or SIA must either assign an FBI employee to conduct the Assessment based upon information contained in the FD-71 or Guardian or close the Assessment. The opening date for Type 1 & 2 Assessments is the date the SSA or SIA assigns an FBI employee to conduct the Assessment. The FBI employee and SSA or SIA must apply the standards for opening or approving a Type 1 & 2 Assessment contained in DIOG Section 5.5.

5.6.3.1.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) As soon as practicable, but not more than five (5) business days after determining the Type 1 & 2 Assessment involves a sensitive investigative matter (SIM), the matter must be reviewed by the CDC and approved by the SAC. The term "sensitive investigative matter" is defined in DIOG Section 5.7 and DIOG Section 10. The FD-71 or Guardian has selection options in the form to designate the Assessment as a "Sensitive Investigative Matter" and to document the required review and approvals.

5.6.3.1.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 1 & 2 Assessments.

5.6.3.1.6 (U) JUSTIFICATION REVIEW

(U//FOUO) If a Type 1 & 2 Assessment is not concluded within 30 days, the SSA or SIA must conduct a justification review every 30 days (recurring until the Assessment is closed) in accordance with DIOG Section 3.4.4.

5.6.3.1.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 1 & 2 Assessment may be conducted by an investigative field office squad or FBIHQ operational division.

5.6.3.1.8 (U) EXAMPLES/SCENARIOS OF TYPE 1 & 2 ASSESSMENTS

5.6.3.1.8.1 (U) EXAMPLE 1

(U//FOUO) Scenario: A series of news articles in May and June report on a shakeup in Gloucester County government. The June 18th front page article was captioned "County Government Hijacked by Board of Supervisors." One of the elected Supervisors (X), according to the story, has a familial relationship to a prominent local developer, who has submitted a zoning request to the county board of supervisors for a 1200 unit residential and golf course community.

(U//FOUO) Response: Without supervisor approval, an FBI employee on the Public Corruption Squad may begin to track the story by conducting routine internal FBI database checks for possible business affiliations, personal family relationships, criminal history, and any references in FBI files to the Developer or the County Supervisor X.

(U//FOUO) The FBI employee can conduct record checks (search FBI/DOJ records, USIC records, any other US government records, state or local records), and Internet searches (whether open-source or paid-for services) without opening an Assessment. Because the FBI employee is reviewing existing information already in its possession or to which it has lawful access, this does not constitute new investigative activity. (See Section 5.1.1) If an employee does not establish an authorized purpose to open an Assessment (or Predicated Investigation) after conducting these records checks or

Internet searches, the FBI employee should refer to Section 5.1.2 above for documenting these activities.

(U//FOUO) Without supervisor approval, the FBI employee may ask an open confidential human source (CHS), whose placement is such that he/she might have relevant knowledge, what he/she knows about the Developer and County Supervisor X. If an Assessment is opened, the FBI employee may also task the CHS (without supervisor approval) to contact the Developer for the purpose of seeking information about the Developer's future project plans. In either instance the FBI employee must ensure that he or she is using the least intrusive method that is reasonable based upon the circumstances of the investigation. Because this is a sensitive investigative matter (domestic public official), as soon as practicable, but not more than five (5) business days after the SIM arises, it must be brought to the CDC for review and to the SAC for approval to continue the Assessment. The initiation date for this type of Assessment is the date the SAC approves the Assessment. The FBI employee must memorialize the contact with the CHS in DELTA and complete an FD-71.

5.6.3.1.8.2 (U) EXAMPLE 2

(U//FOUO) Scenario: An FBI employee receives a telephone call from an anonymous caller who complains about a new émigré Imam at a local mosque. The caller says the Imam has been making radical statements in public and private conversations and has openly invited all male mosque members between the ages of 16 and 40 to join a Wednesday night "awakening" meeting. Afterwards, according to the caller, a few select attendees are chosen to go to another room where, the caller believes, they talk about conducting holy war against the United States.

(U//FOUO) Response: Because this is a terrorism-related item, the FBI employee must enter the information into Guardian and be assigned a Guardian lead by the supervisor. Additionally, because this Assessment involves a sensitive investigative matter (a religious figure), as soon as practicable, but not more than five (5) business days after the SIM arises, this matter must be forwarded to the CDC for review and the SAC for approval. Without supervisor approval, but consistent with the requirement to use the least intrusive method feasible, the FBI employee may also contact a CHS to determine whether the CHS knows or has heard anything about the new Imam. The FBI employee must memorialize the contact in DELTA. Investigative methods used in this Assessment must be documented in Guardian, and if any methods required supervisor approval, those approvals must also be documented in Guardian.

5.6.3.2 (U) TYPE 3 ASSESSMENTS

(U) Type 3 Assessment defined: Identify, obtain and utilize information about actual or potential national security threats or Federal criminal activities, or the vulnerability to such threats or activities. [See AGG-Dom, Part II.A.3.b]

(U//FOUO) Type 3 Assessments may be used to analyze or determine whether particular national security or criminal threats exist within the AOR and whether there are victims or targets within the AOR who are vulnerable to any such actual or potential threats. The

authorized purpose and clearly defined objective(s) of a Type 3 Assessment must be based on or related to actual or potential Federal criminal or national security targets, threats, or vulnerabilities. While no particular factual predication is required, the basis of the Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only such factors.

(U//FOUO) Whenever a Type 3 Assessment identifies and begins to focus on a specific individual(s), group(s) or organization(s), whose activities may constitute a violation of Federal criminal law or a threat to the national security, a separate Type 1 & 2 Assessment or a Predicated Investigation must be opened on that individual, group or organization.

(U//FOUO) A Type 3 Assessment may not be opened based solely upon the existence of a collection requirement, and addressing a collection requirement cannot be the authorized purpose of a Type 3 Assessment. Information obtained during the course of this type of assessment (or any other Assessment or Predicated Investigation) may, however, be responsive to collection requirements and collection requirements may be used to inform and help focus a Type 3 Assessment (or any other Assessment or Predicated Investigation) while also providing information about potential targets, threats and/or vulnerabilities.

(U//FOUO) Investigative activity undertaken during Special Events assessments (such as “Joint Threat Assessments,” “Joint Special Event Threat Assessments,” and “Special Events Threat Assessments”) must be documented using a Type 3 Assessment opened under the relevant investigative classification (e.g., 415, etc) or the 800I classification. Opening a Type 3 Assessment for these events does not eliminate the requirement to use the 300A classification as a control file for administrative functions related to the special event; the 300A control file cannot be used to maintain or upload investigative/Assessment documents.

(U//FOUO) A Type 3 Assessment may not be used for the purpose of collecting positive foreign intelligence, although such intelligence may be incidentally collected. Positive foreign intelligence can only be intentionally collected pursuant to DIOG Sections 5.6.3.5 (Type 6 Assessment) and/or Section 9.

(U//FOUO) See Section 5.11 below for intelligence collection, (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the 815I field office file.

5.6.3.2.1 (U) DURATION

(U//FOUO) A Type 3 Assessment may only be opened with prior supervisor approval. The effective date of the Assessment is the date the final approval authority approves the EC as specified in Section 5.6.2 above. A Type 3 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 3 Assessment is not limited in duration, when the clearly defined objective(s) have been met, the Assessment must be closed with an EC approved by the supervisor.

5.6.3.2.2 (U) DOCUMENTATION

(U//FOUO) The title/caption of the opening EC must contain the word “Assessment,” and the synopsis must identify the authorized purpose and the clearly defined objective(s) of the Assessment. If appropriate, the Details section of the EC may provide more details regarding the authorized purpose and clearly defined objective(s). If additional objectives arise during the course of the Assessment, they must be documented with an EC and approved by the supervisor. If at the time of the opening, or at anytime thereafter, the Assessment involves a sensitive investigative matter, the title/caption must also contain the words “Assessment” and “Sensitive Investigative Matter.” (See DIOG Section 10.4)

(U//FOUO) Additionally, if DIOG Section 18 requires documentation of the approval to use an authorized investigative method in an Assessment, such requests, as well as all uses of those methods, must be documented by an EC.

(U//FOUO) If opened by the DI, a Regional Intelligence Group (RIG), or a Field Intelligence Group (FIG), the Type 3 Assessment must be documented in the appropriate 801I-807I or 815I classification file. A Type 3 Assessment opened by an investigative division or investigative field office squad must be documented in the appropriate investigative classification Assessment file. The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

5.6.3.2.3 (U) APPROVAL

(U//FOUO) All Type 3 Assessments must be approved in advance by a supervisor and opened by EC. Notwithstanding any other provision in the DIOG, a Type 3 Assessment cannot be opened based on oral approval. The supervisor must review and approve a Type 3 Assessment in accordance with the standards set forth in Section 5.5. Additional approval requirements apply to SIMs, as described below.

5.6.3.2.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If the Assessment involves a sensitive investigative matter, the CDC must review and the SAC must approve the Assessment prior to opening. If a SIM arises after the opening of a Type 3 Assessment, Assessment activity may continue, but the matter must be documented in an EC reviewed by the CDC and approved by the SAC as soon as practicable but not more than five (5) business days after the SIM arises. The term “sensitive investigative matter” is defined in DIOG Sections 5.7.1 and Section 10.

(U//FOUO) Investigative methods that may be used in Assessments are set forth in DIOG Section 18.

(U//FOUO) As specified in division PGs, there may be agreements (e.g., Memoranda of Understanding, Treaties) that require additional coordination and approval prior to conducting certain activities.

5.6.3.2.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 3 Assessments.

5.6.3.2.6 (U) FILE REVIEW

(U//FOUO) A Type 3 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.2.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 3 Assessment may be opened and conducted by FIGs, RIGs, the DI, field office investigative squads, and FBIHQ operational divisions. The nature of the Assessment dictates the file classification into which the Type 3 Assessment is opened. Assessments conducted by the DI, FIGs or RIGs must be opened in the appropriate 800I – 807I, or 815I file classifications. All other Assessments must be opened in the appropriate investigative file classification.

5.6.3.2.8 (U) EXAMPLES OF TYPE 3 ASSESSMENTS

5.6.3.2.8.1 (U) EXAMPLE 1

(U//FOUO) Scenario: A state awards substantial grant money from Congress for road improvements over a 10 year period. The local population and business trends do not appear to support a need for such improvements, and the state has a history of corruption in awarding contracts. A review of the newspaper and the Internet shows a pattern of similar awards from the same state office over the past six months.

(U//FOUO) Response: The field office may open a Type 3 Assessment to determine the potential vulnerability of the grant process to corruption (e.g., misdirection of funds or kickbacks to public officials). If the Assessment is likely to obtain information relevant to a SIM as defined in DIOG Section 10 (e.g., possible kickbacks to a domestic public official), the FBI employee must obtain CDC review and SAC approval before opening this assessment, or if the SIM develops after the Assessment is open, such review and approval must be obtained within 5 business days. If while conducting this Assessment information is obtained that addresses a national or field office collection requirement, that information should be disseminated to the appropriate entity.

5.6.3.2.8.2 (U) EXAMPLE 2

(U//FOUO) Scenario: A field office learns, by reading an Intelligence Bulletin, that a foreign intelligence service has recently “stepped up” its efforts to collect technical information about a particular type of avionics equipment. Other available intelligence community products confirm the foreign intelligence service’s interest in the equipment and report that the service has sought to identify engineers of a particular nationality with access to the technology and with possible interest in assisting the development for their former country.

(U//FOUO) *Response:* The field office may open a Type 3 Assessment to determine whether any manufacturers or engineering facilities within its territory produce or contribute to the design or production of the avionics equipment sought and whether they or their employees may be a target of or vulnerable to the foreign intelligence service's attempts to exploit this technology. If while conducting this Assessment information is obtained that addresses a national or field office collection requirement, that information should be disseminated to the appropriate entity.

5.6.3.2.8.3 (U) EXAMPLE 3

(U//FOUO) *Scenario:* Local newspapers report that a number of ethnic restaurants in a field office's territory have recently been vandalized and one restaurant owner has suggested that a non-traditional organized crime group may be trying to extort these restaurants.

(U//FOUO) *Response:* The field office may open a Type 3 Assessment to determine whether the non-traditional organized crime group is trying to establish a presence within the field office's AOR (making businesses in the AOR potential targets of or vulnerable to the group's extortionate behavior). The field office would want to acquire information to determine whether the vandalism is attributed to any organized crime group and whether the vandalism appeared to have a purpose. If such a link is established and a specific group or persons are identified as likely responsible for the vandalism, the field office should determine whether a Type 1 & 2 Assessment or a Predicated Investigation should be opened on those identified subjects. Moreover, if the Assessment obtains information that is responsive to a national or field office collection requirement, that information should be disseminated to the appropriate entity.

5.6.3.2.8.4 (U) EXAMPLE 4

(U//FOUO) *Scenario:* A field office receives an IIR originating from a neighboring field office that identifies an Outlaw Motorcycle Gang (OMG) prominent in the originating office's domain. The receiving office is unaware of any reports or investigations indicating the presence of the particular OMG within its domain, but it would like to know whether the particular OMG has established such a presence. A Type 3 Assessment could be opened to determine whether the particular OMG has established a presence in the receiving field office's domain and the extent to which the office's domain may be a target of or vulnerable to criminal activities of this OMG (e.g., the extent and scope of this threat).

(U//FOUO) *Response:* If, through this Assessment, it is determined that the particular OMG has, is, or is about to engage in criminal activities, and the field office wants to investigate the OMG's criminal activities, it must close the Type 3 Assessment and open a Type 1 & 2 Assessment or a Predicated Investigation on the particular OMG (depending upon the level of predication developed).

(U//FOUO) *Response:* If the Type 3 Assessment was opened to determine whether any outlaw motorcycle gangs were operating within the AOR (rather than to determine whether the specific OMG was operating), and discovers a particular OMG is involved in

criminal activities, the field office would be required to open a Type 1 & 2 Assessment or a Predicated Investigation on that identified particular OMG (depending upon the level of predication). In this scenario, the Type 3 Assessment could remain open, however, to determine whether any other OMGs pose a threat within the domain.

5.6.3.2.8.5 (U) EXAMPLE 5

(U//FOUO) *Scenario:* The annual North American International Auto Show (NAIAS) will take place in a local field office AOR. This event will attract individuals from all over the world. The field office needs to assess whether the special event itself may be a target or victim of Federal criminal violations or national security threats and to what extent other entities within the AOR may be exposed to such crimes or threats.

(U//FOUO) *Response:* To determine whether the event may be a target of or vulnerable to a terrorist attack, a Type 3 Assessment may be opened. If there is adequate information regarding a particular person or group of persons posing a threat to this event, then a Type 1 & 2 Assessment or a Predicated Investigation can also be opened on that specific person or group.

5.6.3.3 (U) TYPE 4 ASSESSMENTS

(U) Type 4 Assessment defined: Obtain and retain information to inform or facilitate intelligence analysis and planning. [AGG-Dom, Part IV]

(U//FOUO) A Type 4 Assessment may be opened to obtain information that informs or facilitates the FBI's intelligence analysis and planning functions. The authorized purpose and clearly defined objective(s) of a Type 4 Assessment must be based on, or related to, the need to collect or acquire information for current or future intelligence analysis and planning purposes. An Assessment under this section, oftentimes referred to as a "domain Assessment," may lead to the identification of intelligence gaps, the development of FBI collection requirements, or the opening of new Assessments or Predicated Investigations.

(U//FOUO) A Type 4 Assessment is not threat specific; threat-based Assessments are opened and governed by DIOG Section 5.6.3.2 (Type 3 Assessment). While no particular factual predication is required for a Type 4 Assessment, the Assessment cannot be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only such factors.

(U//FOUO) Whenever a Type 4 Assessment identifies and begins to focus on specific individual(s), group(s), or organization(s), whose activities may constitute a violation of Federal criminal law or a threat to the national security, a separate Type 1 & 2 Assessment or a Predicated Investigation must be opened. Similarly, if a Type 4 Assessment identifies a particular national security or criminal threat within the AOR, or identifies victims or targets within an AOR who are vulnerable to any actual or potential threat, a separate Type 3 Assessment or Predicated Investigation must be opened.

(U//FOUO) A Type 4 Assessment may not be used for the purpose of collecting positive foreign intelligence (PFI), although such intelligence may be incidentally collected. Positive

foreign intelligence can only be intentionally collected pursuant to DIOG Sections 5.6.3.5 (Type 6 Assessment) and/or Section 9.

(U//FOUO) See Section 5.11 below for intelligence collection, (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the 8151 field office file.

5.6.3.3.1 (U) DURATION

(U//FOUO) A Type 4 Assessment may only be opened with prior supervisor approval. The effective date of the Assessment is the date the final approval authority approves the EC as specified in Section 5.6.2 above. A Type 4 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 4 Assessment is not limited in duration, when the clearly defined objective(s) have been met, the Assessment must be closed with an EC approved by the supervisor.

5.6.3.3.2 (U) DOCUMENTATION

(U//FOUO) The title/caption of the opening EC must contain the word "Assessment," and the synopsis must identify the authorized purpose and the clearly defined objective(s) of the Assessment. If appropriate, the Details section of the EC may provide more details regarding the authorized purpose and clearly defined objective(s). If additional objectives arise during the course of the Assessment, they must be documented with an EC and approved by the supervisor. If at the time of the opening, or at anytime thereafter, the Assessment involves a sensitive investigative matter, the title/caption must contain the words "Assessment" and "Sensitive Investigative Matter."

(U//FOUO) Additionally, if DIOG Section 18 requires documentation of the approval to use an authorized investigative method in an Assessment, such requests, as well as all uses of those methods, must be documented by an EC.

(U//FOUO) This type of Assessment must be documented in the appropriate 818A through F or 815H classification file. The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

5.6.3.3.3 (U) APPROVAL

(U//FOUO) All Type 4 Assessments must be approved in advance by a supervisor and opened by an EC. Notwithstanding any other provision in the DIOG, a Type 4 Assessment cannot be opened based on oral approval. The supervisor must approve a Type 4 Assessment in accordance with the standards discussed in DIOG Section 5.5. Additional approval requirements apply to SIMs, as described below.

5.6.3.3.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If the Assessment involves a sensitive investigative matter (SIM), the CDC must review and the SAC must approve the Assessment prior to opening. If a SIM arises after the opening of a Type 4 Assessment, Assessment activity may continue, but the matter must be

documented in an EC reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five (5) business days after the SIM arises. The term “sensitive investigative matter” is defined in DIOG Section 5.7 and Section 10.

5.6.3.3.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 4 Assessments.

5.6.3.3.6 (U) FILE REVIEW

(U//FOUO) A Type 4 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.3.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 4 Assessment may only be opened by the DI, field office FIGs or Regional Intelligence Groups (RIG).

5.6.3.3.8 (U) EXAMPLES OF TYPE 4 ASSESSMENTS

5.6.3.3.8.1 (U) EXAMPLE 1

(U//FOUO) Scenario: A field office wishes to acquire the following information/data from public records/sources in order to increase its knowledge of its domain so that it can prepare intelligence reports regarding threats: (i) general demographics (e.g., general population to include concentrations of racial and ethnic groups); (ii) physical location of facilities of interest (e.g., hospitals, media outlets, sports arenas, schools, religious facilities, manufacturing facilities, etc.); (iii) types and location of critical infrastructure facilities (e.g., dams, power plants, airports, ports); and (iv) location of military installations and defense contractors. After acquiring this information/data, the field office may store, analyze, map, and share the information as appropriate. All of the information/data can be obtained from public records/sources available to the public, as well as the FBI, by methods authorized before opening an Assessment. (See DIOG Section 5.1.1)

(U//FOUO) Response: Because this information may be obtained from public sources by methods authorized before opening an Assessment as described in DIOG Section 5.1.1, the field office is not required to open a Type 4 Assessment. It may do so, however, if it wishes.

5.6.3.3.8.2 (U) EXAMPLE 2

(U//FOUO) Scenario: Same facts as in example #1 above except the field office needs information about (i) demographics; (ii) criminal activity reports showing the location of certain criminal gang activities; and (iii) information solely in the possession of the Department of Defense (e.g., the location of defense contractors).

(U//FOUO) *Response:* If the information sought from state and local authorities already exists and the information about the location of defense contractors is available in a DOD database, it is not necessary to open a Type 4 Assessment to obtain it. (See DIOG Section 5.1.1) A request of a state or local agency for demographic or criminal activity information which does not exist at the time of the request (and would, therefore, not be considered historical) or a request of DOD for a defense contractor report which had not yet been prepared would require the opening of a Type 4 Assessment.

5.6.3.3.8.3 (U) EXAMPLE 3

(U//FOUO) *Scenario:* A field office wishes to collect information about population demographics within its domain in order to have a better understanding of the composition of the community, the different ethnic groups, religious affiliations, community interests and dynamics, businesses, etc. for analysis and planning.

(U//FOUO) *Response:* In order to obtain this information for analysis and planning, the field office FIG must open a Type 4 Assessment to determine the demographics and population. The field office may: (i) obtain public information; (ii) search/obtain records and information from FBI/DOJ; (iii) search/obtain records or information from other Federal, state, local, tribal or foreign agencies (e.g., I-94 Data, Visa Applications, etc.); (iv) interview identified sources, and liaison contacts; and (v) search on-line services and resources (i.e., commercial databases to identify businesses, organizations, and institutions of interest).

5.6.3.3.8.4 (U) EXAMPLE 4

(U//FOUO) *Scenario:* A field office wishes to gather information pertaining to critical national assets, research facilities, universities, places of worship, bridges, dams, historic buildings and monuments, government facilities, significant private sector facilities, etc., to map the data, in order to better understand key infrastructure components within its AOR.

(U//FOUO) *Response:* In order to obtain this information for analysis and planning, the field office FIG would need to open a Type 4 Assessment because it would require the use of investigative methods described in Section 18. The field office FIG may store, analyze, map, and share the information as set forth in DIOG Sections 12, 14, and 15.

5.6.3.4 (U) TYPE 5 ASSESSMENTS

(U) Type 5 Assessment defined: Seek information to identify potential human sources, assess their suitability, credibility, or value of individuals as human sources.

(U//FOUO) A Type 5 Assessment provides the authority and a mechanism to identify, evaluate and recruit a Potential Confidential Human Source (CHS) prior to opening and operating them as a CHS in DELTA. A Type 5 Assessment is not a prerequisite to opening an individual as an operational CHS in DELTA if the necessary information for opening has been obtained through other methods (e.g., following arrest, an individual agrees to become as CHS).

(U//FOUO) A Type 5 Assessment may be opened:

- A) (U//FOUO) on a specific named individual who is a potential CHS; or
- B) (U//FOUO) without a specific named individual, if the goal is to identify individuals with placement and access to particular information.

(U//FOUO) A Type 5 Assessment may not be opened on a subject of a Predicated Investigation. A previously opened CHS cannot be opened as a Type 5 Assessment.

(U//FOUO) Type 5 Assessment activities may not be based solely on race, ethnicity, national origin, religion, or activities protected by the First Amendment, or a combination of only such factors.

(U//FOUO) There are three phases of a Type 5 Assessment. The phases are: (1) Identification Phase, (2) Evaluation Phase, and (3) Recruitment Phase. A Type 5 Assessment opened on a specific named individual may only use the Evaluation and Recruitment phases as described below. A Type 5 Assessment opened without a specific named individual is limited to the Identification Phase only. Once the Identification Phase has succeeded in identifying specific individuals who might have appropriate placement and access, the FBI employee must open a new separate Type 5 Assessment on any individual the employee wishes to further evaluate and possibly recruit as a CHS. The original Type 5 Assessment without a specific named individual may remain open in the Identification Phase, if the authorized purpose and clearly defined objective(s) still exist.

5.6.3.4.1 (U) PHASES OF TYPE 5 ASSESSMENTS

5.6.3.4.1.1 (U//FOUO) IDENTIFICATION PHASE

(U//FOUO) This phase may be used by an SA assigned to either a HUMINT or investigative squad or by an IA assigned to the field office or FBIHQ to identify potential CHSs who seem likely to have placement and access to information or intelligence related to criminal or national security threats, investigations, or collection requirements without naming a specific individual. The goal of this phase is to identify individuals with CHS potential, who may then be evaluated and recruited under the Evaluation and Recruitment Phases of a Type 5 Assessment.

(U//FOUO) This phase is initiated with the approval of a CHS identification plan. The plan, which must be based on a thorough review of available intelligence regarding the threat, investigation or collection requirement at issue, must specify characteristics of individuals likely to have CHS potential, and the investigative methods (e.g., database searches, surveillance of specific locations, attendance at specific events) that will be used to identify individuals with those characteristics. Selection of characteristics/search criteria must have a logical connection to intelligence or known facts, and may not be based merely on conjecture. In addition, selected characteristics may not be based solely on race, ethnicity, national origin, religion or activities protected under the First Amendment or a combination of only such factors. See DIOG Section 4 for further explanation on the permissible use of race, ethnic identity or activities protected under the First Amendment. The investigative methods that may be used to identify individuals

with the specified characteristics needed must also be based on existing intelligence and be reasonably likely to yield individuals with the specified characteristics.

(U//FOUO) If necessary, after a CHS identification plan has been approved, and a group of individuals who potentially have placement and access to the relevant information have been identified, the SA or IA may, with authorization set forth in Section 5.6.3.4.8, use additional characteristics to narrow the group of individuals to those most likely to have the desired placement and access.

(U//FOUO) Once an SA or IA has narrowed the field to one or more known persons who appear to have potential as CHSs, in order to gather additional information regarding background and authenticity or, in order for an SA to undertake efforts to recruit the individual, a Type 5 Assessment must be opened on the specific named individual(s) in accordance with subsection 5.6.3.4.1.2, below.

5.6.3.4.1.2 (U//FOUO) EVALUATION PHASE

(U//FOUO) This phase may be used by an SA assigned to either a HUMINT or investigative squad or by an IA assigned to the field office or FBIHQ to evaluate a known individual believed to have placement and access so that the individual, if successfully recruited, can provide the FBI with information of value. The goal of this phase of a Type 5 Assessment is to gather information, through the use of the investigative methods set forth in Section 8, below regarding background, authenticity, and suitability of a particular Potential CHS (specific named individual). An IA who develops information during this phase that indicates a Potential CHS is worthy of recruitment should prepare a Source Identification Package (SIP) for use by an SA on the appropriate HUMINT or investigative squad to recruit the individual. If information developed during this phase indicates the individual should not be recruited as a CHS, the Type 5 Assessment must be closed.

5.6.3.4.1.3 (U//FOUO) RECRUITMENT PHASE

(U//FOUO) This phase may only be used by an SA assigned to a HUMINT or investigative squad. The goal of this phase of a Type 5 Assessment is to recruit the potential CHS to become an operational CHS, and therefore, the recruitment phase may focus only on a specific named individual. Information from a SIP or other information/intelligence available to the SA may be used during the recruitment phase. If the recruitment is successful, the Type 5 Assessment must be closed (See Section 5.6.3.4.9, below) and the individual opened as a CHS in DELTA. The Type 5 Assessment must also be closed if the recruitment is not successful, either because the individual declines to become a CHS or a determination is made not to continue the recruitment.

5.6.3.4.2 (U) DURATION

(U//FOUO) The effective date of a Type 5 Assessment is the date the highest level of authority required approves the opening EC (or successor form in DELTA). A Type 5 Assessment may continue for as long as necessary to achieve its authorized purpose and

clearly defined objective(s) as set forth in the three phases above or when it is determined that the individual named subject cannot or should not be recruited as a CHS.

5.6.3.4.3 (U) DOCUMENTATION

5.6.3.4.3.1 (U//FOUO) IDENTIFICATION PHASE

(U//FOUO) The title of the EC (or successor form in DELTA) must read: "Type 5 Assessment, CHS Identification Plan," and contain the number of the appropriate 801R through 807R or 815R file. These sub-files are restricted and consist of numerical classifications corresponding to specific investigative programs. The synopsis must state the authorized purpose and clearly defined objective(s). If at the time of the opening, or at anytime thereafter, the Assessment involves a sensitive investigative matter, the title/caption must also contain the words "Sensitive Investigative Matter." The Details section must outline the operational plan, including the following information:

A) (U//FOUO) The particular placement and access to information that the FBI is seeking, why the FBI is seeking a person with such placement and access, and the file number and title of the Assessment or Predicated Investigation the Type 5 Assessment will support.

(U//FOUO) *Example:* The FBI is seeking a CHS with access to the leadership of the local chapter of the motorcycle gang "Heaven's Devils." The field office has a Type 3 Assessment open to assess the threat from Heaven's Devils but has no human source penetration to assist that Assessment.

B) (U//FOUO) Characteristics/search criteria intended to be used to generate the pool of individuals who might have appropriate placement and access, and the basis for selecting the particular characteristics/search criteria. There must be an articulated reason to believe the characteristics/search criteria will yield individuals likely to have the desired placement and access, and the characteristics/search criteria may not be based solely on race, ethnicity, national origin, religion or activities protected under the First Amendment or a combination of only such factors.

(U//FOUO) *Example:* Existing intelligence regarding Heaven's Devils indicates most members are 30 to 55 years old, male, have visible "Heaven's Devils" tattoos, ride Vespa motorcycles and prefer wine bars as gathering places. A significant percentage of members have a criminal record, typically for possession of user quantities of controlled substances. Accordingly, the CHS identification plan includes identifying middle-aged males who are registered owners of Vespa motorcycles and who have a criminal record. The identification plan also includes ascertaining the social gathering places for local members.

C) (U//FOUO) The investigative methods (e.g., database searches, website monitoring, surveillance of physical locations, attendance at particular events) the IA or SA anticipates using to find individuals and an explanation why these investigative methods are expected to yield persons who are likely to have the needed placement and access.

(U//FOUO) *Example:* An IA develops a plan to search and monitor specific social networking sites known to be used by Heaven's Devils members as a means of identifying members, associates, and contacts who may have value as CHSs. An SA develops a plan to visit local establishments at which Heaven's Devils' members are believed to frequent in order to observe and interact with patrons and staff who may have value as CHSs, or to attend a local

motorcycle expo at which Heaven's Devils' members and vendors are known to patronize or likely to attend.

(U//FOUO) If a Type 5 Assessment has already been opened and an IA or SA wishes to utilize additional characteristics/search criteria or investigative methods in the Identification Phase that were not documented in the opening EC, the additional characteristics/search criteria and/or investigative methods must be documented by EC (or successor form in DELTA). The title must read: "Type 5 Assessment; Modification of CHS Identification Plan." The Details section of the EC must include the additional characteristics/search criteria or investigative methods intended to be used to generate the pool of individuals who might have appropriate placement and access. The EC must also explain the basis for selecting the additional characteristics/search criteria or investigative methods. Selected characteristics/search criteria or investigative methods may not be based solely on race, ethnicity, national origin, religion, or activities protected under the First Amendment or a combination of only such factors.

5.6.3.4.3.2 (U//FOUO) EVALUATION/RECRUITMENT PHASES

(U//FOUO) A Type 5 Assessment opened to evaluate and/or recruit a specific person as a CHS must be opened with an EC (or successor form in DELTA) using the appropriate 801R-807R or 815R file. The 801R-807R or 815R files are restricted files consisting of numerical classifications corresponding to specific investigative programs. The title/caption of the EC must contain the name of the potential CHS and the words "Type 5 Assessment." The synopsis must state the authorized purpose and clearly defined objective(s). The Details section of the EC must provide the facts that indicate the individual has placement and access to information or intelligence related to criminal or national security threats, investigations, or collection requirements, to include the following:

- A) (U//FOUO) The file classification of the Assessment or Predicated Investigation the potential CHS may be able to support;
- B) (U//FOUO) The Potential CHS's date of birth and other available biographical data; and
- C) (U//FOUO) The information to which the person is believed to have placement and access and why such a CHS would be of value to the FBI.

5.6.3.4.4 (U) APPROVAL

(U//FOUO) A Type 5 Assessment must be approved by the appropriate supervisor and opened with an EC (or successor form in DELTA). Notwithstanding any other provision in the DIOG, a Type 5 Assessment cannot be opened on oral approval. For SAs, a Type 5 Assessment must be approved by their SSA. For IAs, a Type 5 Assessment must be approved by the SIA and the SSA on the HUMINT or investigative squad that will potentially recruit the individual. An SSA and/or SIA must use the standards provided in DIOG Section 5.5 when deciding whether to approve a Type 5 Assessment. Additional approval requirements apply to Sensitive Potential CHSs, as described below.

5.6.3.4.4.1 (U//FOUO) SENSITIVE POTENTIAL CHSs AND GROUPS

(U//FOUO) CDC review and SAC approval is required before a Type 5 Assessment may be opened on a Sensitive Potential CHS or if, during the Identification Phase, a sensitive characteristic is at least one aspect being used to identify individuals with potential placement and access to information of interest. If it is determined after opening a Type 5 Assessment that a Potential CHS is Sensitive or that a sensitive characteristic must be added to the Potential CHS Identification Plan, the Assessment activity may continue, but the matter must be documented in an EC (or a successor form in DELTA) and reviewed by the CDC and approved by the SAC as soon as practicable, but not more than 5 business days of this determination. A Sensitive Potential CHS or sensitive characteristic (as part of an Identification Plan) is defined as follows:

- A) (U//FOUO) A domestic public official (other than a member of the U.S. Congress or White House Staff – which requires higher approval authority, see CHSPG for additional details);
- B) (U//FOUO) A domestic political candidate;
- C) (U//FOUO) An individual prominent within a religious organization;
- D) (U//FOUO) An individual prominent within a domestic political organization;
- E) (U//FOUO) A member of the news media; or
- F) (U//FOUO) A member of the faculty or the administration of a college or university in the United States.

(U//FOUO) DIOG Section 10 should be consulted for a definition of these terms.

(U//FOUO) For additional information regarding Sensitive Potential CHSs, see CHSPG, Part 2, & DIOG Section 18.5.3.

5.6.3.4.5 (U) NOTICE

(U//FOUO) There is no requirement to provide notice to FBIHQ or DOJ of opening or closing Type 5 Assessments.

5.6.3.4.6 (U) FILE REVIEW

(U//FOUO) A supervisory file review must be conducted every 90 days (60 days for probationary employees). In addition to the requirements of section 3.4.4.9, the purpose of the file review is to determine the following:

- A) (U//FOUO) Whether authorized investigative methods have been used properly in all phases of the Assessment;
- B) (U//FOUO) Whether, in the Identification Phase, the Assessment has successfully narrowed the field to a group of individuals who are likely to have appropriate placement and access;
- C) (U//FOUO) Whether reimbursable expenses incurred by an SA, if any, were reasonable, properly authorized, and properly documented;
- D) (U//FOUO) Whether the Potential CHS was tasked to provide information or paid for his/her services or expenses (activities which are not permitted prior to opening the person as a CHS);

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- E) (U//FOUO) Whether there is a reasonable likelihood the Potential CHS can and should be recruited or, if the Assessment is in the Identification Phase, the plan has a reasonable likelihood of generating a group of Potential CHSs; and
- F) (U//FOUO) Whether the Type 5 Assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is justified, SIA/SSA must document the rationale for keeping the Type 5 Assessment open.

5.6.3.4.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 5 Assessment without a specific named individual may be opened by SAs on HUMINT squads or IAs assigned the field office FIG or to FBIHQ. A Type 5 Assessment on specific named individual may be opened by SAs on HUMINT or investigative squads, and by IAs assigned to the field office FIG, investigative squads, or to FBIHQ.

5.6.3.4.8 (U) AUTHORIZED INVESTIGATIVE METHODS IN TYPE 5 ASSESSMENTS

(U//FOUO) Only the following investigative methods may be used in a Type 5 Assessment, whether in the identification, evaluation, or recruitment phase. All of these investigative methods may be used by SAs. IA's may only use investigative methods (A) through (E).

- A) (U//FOUO) Public information;
- B) (U//FOUO) Records or information – FBI and DOJ;
- C) (U//FOUO) Records or information – Other Federal, state, local, tribal, or foreign government agencies;
- D) (U//FOUO) On-line services and resources;
- E) (U//FOUO) Information voluntarily provided by governmental or private entities;
- F) (U//FOUO) Use of AFID – with certain approvals required (see CHSPG);
- G) (U//FOUO) CHS use and recruitment;
- H) (U//FOUO) Interview or request information from the public or private entities;
- I) (U//FOUO) Physical surveillance (not requiring a court order);
- J) (U//FOUO) Polygraph examinations (see CHSPG); and
- K) (U//FOUO) Trash Covers (Searches that do not require a warrant or court order).

(U//FOUO) **Note:** Consent Searches are authorized in Assessments.⁵

(U//FOUO) Some investigative methods used during Assessments that may require higher supervisory approval are set forth in DIOG Section 18.5.

(U//FOUO) In addition, as specified in division PGs, there may be agreements (e.g., Memoranda of Understanding, etc.) that require additional coordination and approval prior to conducting certain activities.

⁵ (U//FOUO) The DOJ has opined that Consent Searches are authorized in Assessments, as well as in Predicated Investigations.

(U//FOUO) If DIOG Section 18 requires documentation of the request or the approval to use an authorized investigative method, the request and approval must be documented with an EC (or the successor form in DELTA).

5.6.3.4.9 (U) CLOSING TYPE 5 ASSESSMENTS

(U//FOUO) A Type 5 Assessment must be closed with SIA and SSA approval if it was opened by an IA; or with SSA approval if it was opened by an SA, when:

- A) (U//FOUO) In a Type 5 Assessment opened without a specific named individual, it is determined that the characteristics/search criteria used to identify individuals with placement and access to needed information have not succeeded in identifying such individuals, or the FBI no longer has a need for a CHS with the specified placement and access;
- B) (U//FOUO) The Identification Phase has succeeded in identifying specific named individuals who might have appropriate placement and access. If the FBI wishes to further evaluate and possibly recruit any such identified individuals, a separate Type 5 Assessment must be opened on that person. The original Type 5 Assessment may remain open in the identification phase if the authorized purpose and clearly defined objective still exist;
- C) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, it is determined that the Potential CHS is not a suitable candidate for further evaluation and/or recruitment efforts;
- D) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, SA recruitment efforts are successful and the potential CHS has been opened as a CHS in DELTA; or
- E) (U//FOUO) In a Type 5 Assessment opened on a specific named individual, SA efforts to recruit the potential CHS have been unsuccessful or it is determined that further recruitment efforts are not likely to be successful.

5.6.3.4.10 (U) EXAMPLES OF TYPE 5 ASSESSMENTS

5.6.3.4.10.1 (U//FOUO) EXAMPLES OF A TYPE 5 ASSESSMENT OPENED WITHOUT A SPECIFIC NAMED INDIVIDUAL

(U//FOUO) Example A: A field office has a Type 3 Assessment open on the potential terrorist threat from country Y. Through the Type 3 Assessment, the office has determined that it has no CHSs with placement or access to the sizeable country Y émigré population in the AOR. An IA assigned to the FIG has been assigned to identify persons with placement and access to potential terrorist sympathizers.

(U//FOUO) Response A: The IA's assignment is to locate potential CHSs within the AOR who would be in a position to provide information or intelligence regarding threats that might be coming from country Y. A Type 5 Assessment may not be opened solely to locate and identify Country Y's émigré population within the AOR because such an Assessment would be based solely on the group's national origin. However, existing intelligence indicates that the known terrorists from country Y are male, between the ages 15-20, have attended or presently attend American universities, travel to country Y several times a year and fly into rural airport Z when they travel to country Y. The IA determines that the aforementioned characteristics are likely to yield persons with

placement and access to information or intelligence related to the Type 3 Assessment. The IA opens a Type 5 Assessment without an identified subject titled “Type 5 Assessment: CHS Identification Plan.” The EC must set forth the characteristics/search criteria selected for identifying potential CHSs and the basis for selecting those characteristics/search criteria. The IA must also specify the investigative methods he/she plans to use to identify potential CHSs from this group, such as databases the IA will query to find individuals with the identified characteristics. After the results of the various queries are correlated, the IA identifies several individuals who may have the desired placement and access. The IA must open separate Type 5 Assessment on each of these identified individuals in accordance with sub-section 5.6.3.4.3.1 above, to further evaluate their potential as CHSs.

(U//FOUO) *Example B:* A field office has opened a Type 3 Assessment on the recent infiltration in the AOR of a new street gang identified through IIRs submitted by neighboring field offices. A HUMINT SA is assigned to develop CHSs to provide information regarding the gang’s structure, leadership, members, illegal activities, communications and recruitment strategies, etc.

(U//FOUO) *Response B:* Existing intelligence reflects that members of this gang have been known to wear clothing of specified colors, have identifiable graffiti, and use bowling alleys and certain ethnic restaurants as gathering places. Because the SA’s primary focus is on CHS development, he/she must open a Type 5 Assessment without a specific named individual titled “Type 5 Assessment: CHS Identification Plan.” The EC sets forth these identifiable characteristics and the investigative methods the SA plans to use, the basis for their selection and the locations where he/she plans to interact with such individuals. Through the use of authorized investigative methods set forth in subsection 5.6.3.4.8 above, the SA identifies one individual whom the SA believes has the desired placement and access to gang members and whom the SA believes may, in time, be willing to cooperate. The SA opens a Type 5 Assessment on this specific named individual in accordance with Section A, above, to more fully evaluate him/her and initiate recruitment.

5.6.3.4.10.2 (U//FOUO) EXAMPLES OF TYPE 5 ASSESSMENTS OPENED ON SPECIFIC NAMED POTENTIAL CHSs

(U//FOUO) *Example A:* A field office identifies an emerging threat suggesting that La Cosa Nostra (“LCN”) might be moving into its territory. An IA on the FIG opens a Type 3 Assessment authorizing collection regarding the potential threat posed by LCN to the field office AOR. During the Assessment, the IA learns that a specific individual, who appears to periodically associate with persons who are suspected of being members or associates of LCN, filed for bankruptcy. Intelligence suggests that this person is desperate for money, does not appear to be involved with suspected LCN criminal activities, and may be willing to cooperate with the government.

(U//FOUO) *Response A:* A Type 5 Assessment may be opened on the specific named individual to evaluate his/her potential to become a CHS. Because this Assessment is being opened by an IA on the FIG, it must be approved by the IA’s SIA and an SSA on

...all the Assessment were opened by an SA, the SA would be the sole approving authority.) If the SA determines that the person has placement and access that would be of value, the Type 5 Assessment must be transferred to the appropriate HUMINT or investigative squad. If the person is not a potential source, the CHS is opened in DELTA. If the recruitment is unsuccessful, the Assessment must be closed.

Example B: A field office has a Full Investigation open on a group of individuals from country X believed to be targeting engineers and high-tech workers involved in the production of semiconductor chips. Evidence in the Full Investigation suggests that the individuals from country X are attempting to recruit the engineers and high-tech workers to work for them in exchange for money. During the investigation, an engineer who travels frequently to country X has been identified.

(U//FOUO) Response B: Information developed during the Predicated Investigation may be used to determine whether the engineer should be viewed as a subject of the investigation or a potential CHS. If the engineer is determined to be a subject of the Full Investigation, a Type 5 Assessment may not be opened and the engineer needs to be opened as the target of a Full Investigation. If the primary focus of the FBI's interest is to determine whether the individual may be a potential source, a Type 5 Assessment should be opened to collect information necessary to determine whether the FBI should attempt to recruit the engineer as a CHS.

(U//FOUO) If the Assessment is opened by an SA: The SA may open a Type 5 Assessment with his/her SSA approval. If the recruitment is successful, the Type 5 Assessment must be closed when the CHS is opened in DELTA. If the recruitment is unsuccessful, the Type 5 Assessment must be closed.

(U//FOUO) If the Assessment is opened by an IA: The IA must obtain the approval of his/her SSA and the supervisor of the relevant investigative or HUMINT squad to open a Type 5 Assessment. (Note: An IA may not open an individual as a CHS in DELTA.) If the Assessment determines the person has placement and access to information or intelligence that would be of value, the Type 5 Assessment must be transferred to the appropriate investigative squad or the HUMINT squad to further evaluate and recruit the potential CHS.

5.6.3.5 (U) TYPE 6 ASSESSMENTS

(U) Type 6 Assessment defined: Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.

(U//FOUO) A Type 6 Assessment is designed to allow the FBI to determine whether the circumstances within a field office's territory would enable the office to conduct a Full Investigation to collect information responsive to a Positive Foreign Intelligence (PFI) requirement. PFI requirements are described in DIOG Section 9.1. A Type 6 Assessment

the appropriate investigative or HUMINT squad. (If the Assessment were opened by an SA on an investigative squad, then his/her SSA would be the sole approving authority.) If the IA determines during the identification phase that the person has placement and access that would be of value, the Type 5 Assessment must be transferred to the appropriate HUMINT or investigative squad to further evaluate and recruit the potential CHS. If the recruitment is successful, the Type 5 Assessment must be closed when the CHS is opened in DELTA. If the recruitment is unsuccessful, the Assessment must be closed.

(U//FOUO) *Example B:* A field office has a Full Investigation open on a group of individuals from country X believed to be targeting engineers and high-tech workers involved in the production of semiconductor chips. Evidence in the Full Investigation suggests that the individuals from country X are attempting to recruit the engineers and high tech workers to steal information regarding the semiconductor chips in exchange for money. During the investigation, an engineer who travels frequently to country X has been identified.

(U//FOUO) *Response B:* Information developed during the Predicated Investigation may be used to determine whether the engineer should be viewed as a subject of the investigation or a potential CHS. If the engineer is determined to be a subject of the Full Investigation, a Type 5 Assessment may not be opened and the engineer needs to be opened as the target of a Full Investigation. If the primary focus of the FBI's interest is to determine whether the individual may be a potential source, a Type 5 Assessment should be opened to collect information necessary to determine whether the FBI should attempt to recruit the engineer as a CHS.

(U//FOUO) *If the Assessment is opened by an SA:* The SA may open a Type 5 Assessment with his/her SSA approval. If the recruitment is successful, the Type 5 Assessment must be closed when the CHS is opened in DELTA. If the recruitment is unsuccessful, the Type 5 Assessment must be closed.

(U//FOUO) *If the Assessment is opened by an IA:* The IA must obtain the approval of his/her SIA and the supervisor of the relevant investigative or HUMINT squad to open a Type 5 Assessment. (Note: An IA may not open an individual as a CHS in DELTA.) If the Assessment determines the person has placement and access to information or intelligence that would be of value, the Type 5 Assessment must be transferred to the appropriate investigative squad or the HUMINT squad to further evaluate and recruit the potential CHS.

5.6.3.5 (U) TYPE 6 ASSESSMENTS

(U) Type 6 Assessment defined: Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements.

(U//FOUO) A Type 6 Assessment is designed to allow the FBI to determine whether the circumstances within a field office's territory would enable the office to conduct a Full Investigation to collect information responsive to a Positive Foreign Intelligence (PFI) requirement. PFI requirements are described in DIOG Section 9.1. A Type 6 Assessment

focuses on a field office's capability to collect on those PFI requirements. While no particular factual predication is required, the basis of the Assessment cannot be arbitrary or groundless speculation, nor can the Assessment be based solely on the exercise of First Amendment protected activities or on race, ethnicity, national origin or religion, or a combination of only those factors.

(U//FOUO) Foreign Intelligence is "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons." The FBI defines a PFI requirement as a collection requirement issued by the USIC and is accepted by the FBI DI that seeks to collect information outside the FBI's core national security mission.

(U//FOUO) FBI employees must prioritize collection in response to FBI national collection requirements before attempting to collect against a positive foreign intelligence collection requirement. The IPG furnishes guidance on the prioritization of collection.

(U//FOUO) See Section 5.11 below for intelligence collection, (i.e., incidental collection) and documentation requirements. All incidental collection must be documented in the 815I field office file.

5.6.3.5.1 (U) DURATION

(U//FOUO) There are no time limitations on the duration of a Type 6 Assessment. The effective date of the Assessment is the date on which the DI – Domain Collection and HUMINT Management Section (DCHMS), Domain Collection Program Management Unit (DCPMU), UC approves the EC. See DIOG section 5.6.2 above. A Type 6 Assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s). Although a Type 6 Assessment is not limited in duration, when the authorized purpose and clearly defined objective(s) have been met, the Assessment must be closed or converted to a Full Investigation with an EC approved by the field office SSA or SIA and the DCPMU UC. When closing a Type 6 Assessment that is designated as a SIM, the SAC and the DCHMS SC must approve the closing EC.

5.6.3.5.2 (U) DOCUMENTATION

(U//FOUO) A Type 6 Assessment must be opened by EC, using the appropriate 809-814 or 816 file classification. The title/caption of the opening EC must contain the word "Assessment," and the synopsis must identify the authorized purpose and the clearly defined objective(s) of the Assessment. The authorized purpose and clearly defined objective(s) should be described in more detail in the Details section of the EC. If additional objectives arise during the course of the Assessment, they must also be documented in an EC and approved by the field office SSA or SIA. If at the time of the opening, or at anytime thereafter, the Assessment involves a SIM, the title/caption must contain or be changed to also include the words "Assessment" and "Sensitive Investigative Matter."

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

5.6.3.5.3 (U) APPROVAL

(U//FOUO) All Type 6 Assessments must be opened by EC and approved in advance by an SSA or SIA and the appropriate DI UC. A Type 6 Assessment must be approved in accordance with the standards provided in DIOG Section 5.5. Notwithstanding any other provision in the DIOG, a Type 6 Assessment cannot be opened on oral approval.

5.6.3.5.4 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) If a Type 6 Assessment involves a sensitive investigative matter, the CDC/OGC must review and the SAC and the appropriate DI SC must approve the Assessment prior to opening. If a sensitive investigative matter arises after the opening of a Type 6 Assessment, Assessment activity may continue, but the matter must be reviewed by the CDC and approved by the SAC and the DCHMS SC, as soon as practicable, but not more than five (5) business days after the sensitive investigative matter arises. The term “sensitive investigative matter” is defined in DIOG Section 5.7 and Section 10.

5.6.3.5.5 (U) NOTICE

(U//FOUO) FBIHQ authority, as specified above, is required to open a Type 6 Assessment; the opening EC will serve as notice to the DI. There is no requirement to provide notice to DOJ of opening or closing a Type 6 Assessment.

5.6.3.5.6 (U) FILE REVIEW

(U//FOUO) A Type 6 Assessment requires file reviews in accordance with DIOG Section 3.4.4.

5.6.3.5.7 (U) RESPONSIBLE ENTITY

(U//FOUO) A Type 6 Assessment may only be opened and conducted by the FIG and the DI (Refer to IPG for further details). Under the management of the FIG, field office investigative squads or FBIHQ divisions may support the collection of information in a Type 6 Assessment.

5.6.3.5.8 (U) EXAMPLES/SCENARIOS OF TYPE 6 ASSESSMENTS

5.6.3.5.8.1 (U) EXAMPLE 1

(U//FOUO) *Example 1:* A field office learns that the exiled leader of the opposition party from a country on the Threat Country List (TCL) is living in the area. The FBI-DI has accepted a USIC collection requirement seeking information about the opposition group’s level of influence in the government-controlled oil industry and published it to the FBI as a PFI collection requirement. The FBI’s core national security mission does not include domestic politics or infrastructure of the TCL country; however, the field office believes it may be uniquely positioned to collect intelligence on this PFI collection requirement.

(U//FOUO) *Response*: The field office may request the DCPMU to authorize a Type 6 Assessment to proceed with initial activity that will determine whether the field office can, in fact, collect against the published PFI collection requirement. The Type 6 Assessment will allow the field office to use the appropriate investigative methods to determine its collection capabilities related to the PFI collection requirement. If the field office determines that it can collect the foreign intelligence, it should contact the DCPMU for authorization to open a Full PFI Investigation. (Refer to DIOG section 9 and IPG for further details.)

5.6.3.5.8.2 (U) EXAMPLE 2

(U//FOUO) *Example 2*: A field office identifies a series of requirements in a National HUMINT Collection Directive (NHCD) related to a designated international terrorist group known to conduct attacks against U.S. interests. The field office believes that there may be a collection opportunity in its territory and requests the DCPMU to authorize a Type 6 Assessment to permit the field office to evaluate its ability to respond to this NHCD.

(U//FOUO) *Response*: A request to open this Type 6 Assessment would not be approved by the DCPMU. A Type 6 Assessment cannot be opened on the ability to collect intelligence on NHCDs unless those NHCDs have been “accepted” and published by the FBI-DI as PFI collection requirements. In addition, these NHCDs would not be “accepted” by the FBI-DI because the neutralization and investigation of terrorist entities, particularly in the U.S., is part of the FBI’s core national security mission, and would not meet the definition of PFI collection requirements. If the field office believes that there may be collection opportunities related to a terrorist group, it should consider opening a Type 3 Assessment to determine whether the group poses a threat in the field office’s AOR.

5.7 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ASSESSMENTS

(U//FOUO) The title/caption of the opening or subsequent EC for an Assessment involving a SIM must contain the words “Assessment” and “Sensitive Investigative Matter.” DIOG Section 10 contains the required approval authority and factors for consideration when determining whether to open or approve an Assessment involving a SIM.

5.7.1 (U) SIM CATEGORIES IN ASSESSMENTS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an Assessment, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary. DIOG Section 10 and the DIOG classified Appendix G define domestic public official, domestic political candidate, religious or domestic political organization, or individual prominent in such an organization, news media, and academic nexus.

(U//FOUO) If at the time of the opening, or at anytime thereafter, an Assessment involves a SIM, the title/caption must contain the words "Assessment" and "Sensitive Investigative Matter."

5.7.2 (U) ACADEMIC NEXUS IN ASSESSMENTS

(U//FOUO) As a matter of FBI policy, an investigative activity having an "academic nexus" is considered a SIM if:

- A) (U//FOUO) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under Assessment is related to the individual's position at the institution; or
- B) (U//FOUO) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of "academic freedom" (e.g., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a SIM even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

5.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD

(U//FOUO) Prior to opening or approving the use of an authorized investigative method, an FBI employee or approving official must determine whether:

- A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose and clearly defined objective(s) of the Assessment;
- B) (U//FOUO) The investigative method selected is the least intrusive method reasonable based upon the circumstances of the investigation;
- C) (U//FOUO) The anticipated value of the Assessment justifies the use of the selected investigative method or methods;
- D) (U//FOUO) If the purpose of the Assessment is to collect positive foreign intelligence, the investigative method complies with the AGG-Dom requirement that the FBI operate openly and consensually with an USPER, to the extent practicable; and
- E) (U//FOUO) The investigative method is an appropriate use of personnel and financial resources.

5.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS**5.9.1 (U) TYPE 1 THROUGH 4 AND TYPE 6 ASSESSMENTS**

(U//FOUO) A complete discussion of these investigative methods, including approval requirements, is contained in DIOG Section 18. The use or dissemination of information obtained by the use of the below-methods must comply with the AGG-Dom and DIOG Section 14. Only the following investigative methods are authorized in Type 1 through 4 and Type 6 Assessments:

- A) (U) Public information. (Section 18.5.1)
- B) (U) Records or information - FBI and DOJ. (Section 18.5.2)
- C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3)
- D) (U) On-line services and resources. (Section 18.5.4)
- E) (U) CHS use and recruitment. (Section 18.5.5)
- F) (U) Interview or request information from the public or private entities. (Section 18.5.6)
- G) (U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)
- H) (U) Physical Surveillance (not requiring a court order). (Section 18.5.8)
- I) (U) Grand jury subpoenas – for telephone or electronic mail subscriber information only (**only available in a Type 1 & 2 Assessment**). (Section 18.5.9)

(U//FOUO) **Note:** Consent Searches are authorized in Assessments.

5.9.2 (U) TYPE 5 ASSESSMENTS

(U//FOUO) In addition to those investigative methods listed above in 5.9.1(A) – (H), Type 5 Assessments only may also use the following investigative methods:

- A) (U) Use of AFID – with certain approvals required. (See CHSPG)
- B) (U) Polygraph Examinations (See CHSPG)
- C) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)

5.10 (U) OTHER INVESTIGATIVE METHODS NOT AUTHORIZED DURING ASSESSMENTS

(U//FOUO) Additional investigative methods, which are authorized for Predicated Investigations, may not be used in Assessments.

5.11 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements, and FBI field office collection requirements may be collected incidental to an Assessment or Predicated Investigation. When information that is responsive to these requirements is incidentally collected in an Assessment or Predicated Investigation, it should be forwarded to the Field Intelligence Group (FIG) for evaluation and potential dissemination

against collection requirements. (See DIOG Section 15.6.1.2 - Written Intelligence Products) All incidental collection must be documented in the 815I field office file.

(U//FOUO) Prior to submitting to the FIG any information that may be evidentiary and therefore potentially discoverable, the FBI employee should discuss with the CDC or OGC the potential impact disseminating the information in an intelligence product may have on the prosecution of the investigation. To the extent dissemination might or is likely to have an adverse impact on the prosecution, the FBI, in consultation with the prosecuting attorney, must assess whether the need for dissemination outweighs the probable impact the dissemination may have on the prosecution.

5.12 (U) RETENTION AND DISSEMINATION OF PRIVACY ACT RECORDS

(U//FOUO) The Privacy Act restricts the maintenance of records relating to the exercise of First Amendment rights by individuals who are USPERs. Such records may be maintained if the information is pertinent to and within the scope of authorized law enforcement activities or for which there is otherwise statutory authority for the purposes of the Privacy Act (5 U.S.C. § 522a[e][7]). Activities authorized by the AGG-Dom are authorized law enforcement activities. Thus, information concerning the exercise of First Amendment rights by USPERs may be retained if it is pertinent to or relevant to the FBI's law enforcement or national security activity. Relevancy must be determined by the circumstances. If the information is not relevant to the law enforcement activity being conducted, then it may not be retained. For more information see DIOG Section 4.1. (AGG-Dom, Part I.C.5)

(U) The Privacy Act, however, may not exempt from disclosure information gathered by the FBI during Positive Foreign Intelligence Assessments (Type 6 Assessments) and investigations of qualified U.S. citizens or lawfully admitted permanent residents if personally identifying information about such persons resides in those files. FBI employees should therefore be particularly vigilant about properly classifying any such information and should avoid unnecessary references to, and the documentation of, identifying information about U.S. citizens and lawfully admitted permanent residents in Positive Foreign Intelligence files. See DIOG Section 4.1.3.

(U//FOUO) Even if information obtained during an Assessment does not warrant opening a Predicated Investigation, the FBI may retain personally identifying information for criminal and national security purposes. In this context, the information may eventually serve a variety of valid analytic purposes as pieces of the overall criminal or intelligence picture are developed to detect and disrupt criminal and terrorist activities. In addition, such information may assist FBI personnel in responding to questions that may subsequently arise as to the nature and extent of the Assessment and its results, whether positive or negative. Furthermore, retention of such information about an individual collected in the course of an Assessment will alert other divisions or field offices considering conducting an Assessment on the same individual that the particular individual is not a criminal or national security threat. As such, retaining personally identifying information collected in the course of an Assessment will also serve to conserve resources and prevent the initiation of unnecessary Assessments and other investigative activities.

5.12.1 (U) MARKING CLOSED ASSESSMENTS THAT CONTAIN PERSONAL INFORMATION

(U) Information obtained during an Assessment that has insufficient value to justify further investigative activity may contain personal information. As a result: (i) when records retained in an Assessment specifically identify an individual or group whose possible involvement in criminal or national security-threatening activity was checked out through the Assessment; and (ii) the Assessment turns up no sufficient basis to justify further investigation of the individual or group, then the records must be clearly annotated as follows:

(U) “It is noted that the individual or group identified during the Assessment does not warrant further FBI investigation at this time. Any dissemination of information from this Assessment regarding the individual or group identified must include an appropriate caveat with the shared information. It is recommended that this Assessment be closed.”

(U) Extreme care should be taken when disseminating personally identifiable information collected during an Assessment that does not lead to sufficient facts to open a Predicated Investigation. If personal information from the Assessment is disseminated outside the FBI according to authorized dissemination guidelines and procedures, it must be accompanied by the required annotation that the Assessment involving this individual or group did not warrant further investigation by the FBI at the time the Assessment was closed.

5.12.1.1 (U) TYPE 1 & 2 ASSESSMENTS

(U//FOUO) When closing Type 1 & 2 Assessments and uploading to a zero classification file, the above statement will be automatically annotated to the FD-71 or Guardian record.

5.12.1.2 (U) TYPE 3, 4, AND 6 ASSESSMENTS

(U//FOUO) When closing Types 3, 4, and 6 Assessments, the language in 5.12.1 above must be included in the synopsis section of the closing EC. Moreover, any FBI employee who shares information from such a closed Assessment file must ensure the following caveat is included in the dissemination:

(U) “This person [or group] was identified during an Assessment but no information was developed at that time that warranted further investigation of the person [or group].”

5.12.1.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) When closing Type 5 Assessments, the language in 5.12.1 above must be included in the synopsis section of the closing EC. Moreover, any FBI employee who shares information from such a closed Assessment file must ensure the following caveat is included in the dissemination:

(U) “This person [or group] was identified during an Assessment to identify potential human sources but the person [or group] did not warrant further development as a source at that time.”

5.13 (U) ASSESSMENT FILE RECORDS MANAGEMENT AND RETENTION

(U//FOUO) Type 1 & 2 Assessments must be maintained in an applicable zero sub-assessment file (e.g., 91-0-ASSESS-D, 15-0-ASSESS) or unaddressed work file. Zero sub-assessment files exist for all investigative classifications and must be used to store all information acquired during these Assessments. Assessments may not be placed in control files or administrative files. When completing the FD-71 or Guardian lead for an Assessment involving a sensitive investigative matter, the FBI employee must select the option “Sensitive Investigative Matter.” Action leads can be set when using a zero sub-assessment file in situations where a prompt checking of information requires action in another division or field office to determine whether a Predicated Investigation is warranted. Records must be retained according to National Archives and Records Administration (NARA) approved disposition authorities.

(U//FOUO) Guardian will be used for documenting only those Assessments described in Section 5.6.3.1 regarding international terrorism, domestic terrorism, weapons of mass destruction terrorism, and cyber terrorism. Guardian provides the ability to set action leads. The retention of records in Guardian, or any successor information technology system, must be retained according to NARA-approved disposition authorities. Consult the RMD Help Desk for assistance.

(U//FOUO) Type 3, 4, 5, and 6 Assessments must have an opening EC. The title/caption of the opening EC must contain the word “Assessment,” and the synopsis must identify the authorized purpose and the clearly defined objective(s) of the Assessment. Assessments may not be placed in control files or administrative files. If at the time of the opening, or at anytime thereafter, the Assessment involves a sensitive investigative matter, the title/caption must also contain the words “Assessment” and “Sensitive Investigative Matter.” When the authorized purpose and objective(s) have been met, a closing EC must be approved by the SSA or SIA and uploaded to the file. If additional objectives arise during the Assessment, they must be documented in an EC, approved by the SSA or SIA, and uploaded to the file. Assessment classification files must be retained according to NARA-approved disposition authorities.

5.14 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

(U//FOUO) To facilitate compliance within an existing investigative program, the FBI employee should consult the relevant division’s PG. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

This Page is Intentionally Blank.

6 (U) PRELIMINARY INVESTIGATIONS

6.1 (U) OVERVIEW

(U) The AGG-Dom authorizes a second level of investigative activity—Predicated Investigations. Predicated Investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations (PI) and Full Investigations (Full). A Preliminary Investigation may be opened on the basis of any “allegation or information” indicative of possible criminal activity or threats to the national security.

6.2 (U) PURPOSE AND SCOPE

(U//FOUO) A Preliminary Investigation may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. However, a Preliminary Investigation cannot be opened or used solely for the purpose of collecting against Positive Foreign Intelligence (PFI) requirements, or for conducting an Enterprise Investigation (EI).

(U) The purposes for conducting Preliminary Investigation include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; obtaining evidence needed for prosecution; or identifying threats to the national security.

(U) The investigation of threats to the national security may constitute an exercise of the FBI’s criminal investigation authority as well as its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes and arresting and prosecuting the perpetrators are likely objectives of investigations relating to threats to the national security. These investigations, however, serve important purposes outside the ambit of normal criminal investigations, by providing the basis for decisions concerning other measures needed to protect the national security.

6.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to protect civil liberties in the conduct of criminal and national security investigations, every Preliminary Investigation under this subsection must have adequate predication that is documented in the opening communication.

(U) No investigative activity, including Preliminary Investigations, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors. Preliminary Investigations of individuals, groups or organizations must focus on activities related to the threats and or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the subject. In this context, it is particularly important

clearly to identify and document the law enforcement or national security basis of the Preliminary Investigation.

(U) *Example:* Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. A Preliminary Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom present investigators with a number of authorized investigative methods in the conduct of a Preliminary Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat.

(U) By emphasizing the use of the least intrusive means to obtain intelligence, information, and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation — means from the available options to obtain the intelligence, information or evidence. (See DIOG Section 4.4).

6.4 (U) LEGAL AUTHORITY

6.4.1 (U) CRIMINAL INVESTIGATIONS

(U) The FBI has statutory authority to investigate all federal crime not assigned exclusively to another federal agency. (See 28 U.S.C. § 533; 18 U.S.C. § 3052; 28 C.F.R. § 0.85 [a])

(U) The FBI also has special investigative jurisdiction to investigate violations of state law in limited circumstances. Specifically, the FBI has jurisdiction to investigate felony killings of state law enforcement officers (28 U.S.C. § 540), violent crimes against interstate travelers (28 U.S.C. § 540A), and serial killers (28 U.S.C. § 540B). Authority to investigate these matters is contingent on receiving a request by an appropriate state official.

6.4.2 (U) THREATS TO THE NATIONAL SECURITY

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See Appendix B: Executive Order (EO) 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.)

(U) “Threats to the national security” are specifically defined to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with EO 12333 or any successor order. (AGG-Dom, Part VII.S)

6.5 (U) PREDICATION

(U) A Preliminary Investigation may be opened on the basis of “information or an allegation” indicating the existence of a circumstance described as follows:

- A) (U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information or intelligence relating to the activity or the involvement or role of an individual, group, or organization in such activity. (AGG-Dom, Part II.B.3)
- B) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information or intelligence that would help to protect against such activity or threat. (AGG-Dom, Part II.B.3)

(U//FOUO) Examples: The following examples have sufficient predication to open a Preliminary Investigation:

- A) (U//FOUO) A CHS, with no established history, alleges that an individual is a member of a terrorist group; this “allegation” is sufficient predication to open a Preliminary Investigation; and
- B) (U//FOUO) If an analyst, while conducting an assessment, discovers on a blog a threat to a specific person, this “information” is enough to open a Preliminary Investigation.

6.6 (U) STANDARDS FOR OPENING OR APPROVING A PRELIMINARY INVESTIGATION

(U) Before opening or approving the conduct of a Preliminary Investigation, an FBI employee or approving official must determine whether:

- A) (U//FOUO) Adequate predication exist for opening a Preliminary Investigation;
- B) (U//FOUO) The Preliminary Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and
- C) (U//FOUO) The Preliminary Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Preliminary Investigations involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in to DIOG Appendix G – Classified Provisions [No Foreign Policy Objection].

(U//FOUO) A Preliminary Investigation cannot be opened based solely on an FBI collection requirement.

6.7 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, NOTICE, EXTENSION, PENDING INACTIVE STATUS, CONVERSION, AND FILE REVIEW

6.7.1 (U) OPENING DOCUMENTATION

(U//FOUO) The predication to open a Preliminary Investigation must be documented in the opening Electronic Communication (EC). The appropriate approving authority may grant oral authority to open a Preliminary Investigation if the standards for opening or approving a Preliminary Investigation are met. Should oral authorization to conduct a Preliminary Investigation be granted, an EC setting forth the predicated facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//FOUO) If at the time of the opening, or at anytime thereafter, the Preliminary Investigation involves a sensitive investigative matter, the title/caption must contain the words "Sensitive Investigative Matter."

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

6.7.1.1 (U) APPROVAL / EFFECTIVE DATE / NOTICE

(U//FOUO) The effective date of the Preliminary Investigation is the date the final approval authority (e.g., Supervisory Special Agent (SSA) or Special Agent-in-Charge (SAC)) approves the EC by electronic signature/date generated by Sentinel or by handwriting their initials and date on the EC. If the Preliminary Investigation is opened on oral authority, the date on which the oral authority was granted is the effective date. See DIOG Section 3.4.2.2. Adding another subject after opening the Preliminary Investigation does not change the original effective date or the extension date.

- A) (U//FOUO) Opened By a Field Office: The opening of a Preliminary Investigation by the field office requires prior approval of the SSA. The opening of a Preliminary Investigation does not require FBI Headquarters (FBIHQ) or Department of Justice (DOJ) notification unless the Preliminary Investigation involves a sensitive investigative matter (SIM) as discussed in paragraph C below. FBIHQ division PGs may, however, require written notification to the appropriate FBIHQ unit and section within 15 calendar days following the opening of Preliminary Investigations.
- B) (U//FOUO) Opened By FBIHQ: The opening of a Preliminary Investigation by FBIHQ requires prior approval of the Unit Chief (UC) with written notification to any applicable field office, within 15 calendar days following the opening. The opening of a Preliminary Investigation does not require DOJ notification unless the Preliminary Investigation involves a SIM as discussed in paragraph C below.
- C) (U//FOUO) Sensitive Investigative Matters (SIM): The opening of a Preliminary Investigation involving a SIM:
 - 1) (U//FOUO) SIM Opened by a Field Office: requires prior Chief Division Counsel (CDC) review and SAC approval, and written notification (EC and a disseminable Letterhead Memorandum (LHM)), to the appropriate FBIHQ operational UC and Section Chief (SC)

within 15 calendar days following the opening. Additionally, the field office must notify the United States Attorney's Office (USAO), in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the United States Attorney (USA)) or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the exceptions described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division or NSD official as soon as practicable, but no later than 30 calendar days after the investigation is opened. The notice must identify all known SIMs involved in the investigation (see DIOG Appendix G - Classified Provisions for additional notice requirements). If a SIM arises after the opening of a Preliminary Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided as specified above.

- 2) (U//FOUO) ***SIM Opened by FBIHQ:*** requires prior OGC review and SC approval, and written notification (an EC and disseminable LHM) to any appropriate field office within 15 calendar days following the opening; the USAO, unless such notification is inappropriate under the circumstances, (e.g., a public corruption investigation of a person who is personally close to the USA) or the matter is a counterintelligence or espionage investigation; and the appropriate DOJ Criminal Division or NSD official, as soon as practicable, but no later than 30 calendar days after the investigation is opened. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, FBIHQ must explain those circumstances in the written notice to the field office(s) and DOJ. The notice must identify all known SIMs involved in the investigation (see DIOG Appendix G - Classified Provisions for additional notice requirements). If a SIM arises after the opening of a Preliminary Investigation, investigative activity may continue, but the matter must be reviewed by OGC and approved by the appropriate FBIHQ operational SC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided as specified above.

- D) (U//FOUO) ***FBIHQ Disapproves Opening:*** The Executive Assistant Director (EAD) for the National Security Branch must notify the Deputy Attorney General if FBIHQ disapproves a field office's opening of a Preliminary Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the National Security Branch is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

6.7.2 (U) EXTENSION

(U//FOUO) A Preliminary Investigation must be concluded within six months of its opening but may be extended for up to six months by the SAC (delegable to the ASAC)⁶. FBIHQ division PGs may require written notification of this six month extension to the appropriate FBIHQ operational unit and section. Extensions of Preliminary Investigations beyond a year are discouraged and may only be approved by the appropriate FBIHQ operational section for "good cause." (AGG-Dom, Part II.B.4.a.ii)

⁶ (U//FOUO) SAC approval required to extend Preliminary Investigations was non-delegable in the previous version of the DIOG. That restriction has been removed in this version.

6.7.2.1 (U) GOOD CAUSE

(U//FOUO) The following factors must be used to determine whether “good cause” exists to extend the Preliminary Investigation beyond one year:

- A) (U//FOUO) Whether logical investigative steps have yielded information that tends to inculcate or exculpate the subject;
- B) (U//FOUO) The progress that has been made toward determining whether a Full Investigation should be opened or the Preliminary Investigation should be closed;
- C) (U//FOUO) Whether, based on the planned course of investigation for the following six months, it is reasonably likely that information will be obtained that will lead to predication for a Full Investigation, thereby warranting an extension for another six months, or will lead to exculpatory information, thereby warranting closing the Preliminary Investigation; and
- D) (U//FOUO) Whether adequate predication has been developed to justify opening a Full Investigation or whether sufficient information has been developed that justifies closing the Preliminary Investigation.

6.7.3 (U) PENDING INACTIVE STATUS

(U//FOUO) The DIOG does not authorize placing Preliminary Investigations into a “pending inactive” status.

6.7.4 (U) CONVERSION TO FULL INVESTIGATION

(U//FOUO) When converting a Preliminary Investigation to a Full Investigation, see DIOG Section 7 for approval and notification requirements.

6.7.5 (U) FILE REVIEW

(U//FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

6.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN PRELIMINARY INVESTIGATIONS

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee or approving official must determine whether:

- A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Preliminary Investigation;
- B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation; and
- C) (U//FOUO) The method to be used is an appropriate use of personnel and financial resources.

6.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) All lawful methods may be used in a Preliminary Investigation, except for mail opening, physical search requiring a Federal Rules of Criminal Procedure (FCRP) Rule 41 search warrant or a Foreign Intelligence Surveillance Act (FISA) order, electronic surveillance requiring a judicial order or warrant (Title III or FISA), or Title VII FISA requests. Authorized methods include, but are not limited to, those listed below. Some of the methods listed are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.4.A)

(U//FOUO) A complete discussion of these investigative methods, including approval requirements, is contained in Section 18. The use or dissemination of information obtained by the use of the below methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in Preliminary Investigations:

- A) (U) Public information. (See Section 18.5.1)
- B) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
- C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
- D) (U) On-line services and resources. (See Section 18.5.4)
- E) (U) CHS use and recruitment. (See Section 18.5.5)
- F) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
- G) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
- H) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- I) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)

(U//FOUO) *Note:* For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an Otherwise Illegal Activity (OIA). Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an Assistant Special Agent-in-Charge (ASAC) or Supervisory Special Agent (SSA).
- (U//FOUO) See the classified provisions in Appendix G for additional information.
- J) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
- K) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
- L) (U) Administrative subpoenas. (See Section 18.6.4)
- M) (U) Grand jury subpoenas. (See Section 18.6.5)
- N) (U) National Security Letters. (See Section 18.6.6)
- O) (U) FISA Order for business records. (See Section 18.6.7)

- P) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)⁷
- Q) (U) Pen registers and trap/trace devices. (See Section 18.6.9)
- R) (U) Mail covers. (See Section 18.6.10)
- S) (U) Polygraph examinations. (See Section 18.6.11)
- T) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)
- U) (U) Undercover operations. (See Section 18.6.13)

(U) See the classified provisions in DIOG Appendix G for additional information.

6.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN PRELIMINARY INVESTIGATIONS

(U//FOUO) The title/caption of the opening or subsequent EC for a Preliminary Investigation involving a SIM must contain the words “Sensitive Investigative Matter.” DIOG Section 10 contains the required approval authority and factors for consideration when determining whether to conduct or approve a Preliminary Investigation involving a SIM.

6.10.1 (U) SIM CATEGORIES IN PRELIMINARY INVESTIGATIONS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, news media, and academic nexus.

6.10.2 (U) ACADEMIC NEXUS IN PRELIMINARY INVESTIGATIONS

(U//FOUO) As a matter of FBI policy, an investigative activity having an “academic nexus” is considered a SIM if:

- A) (U//FOUO) The investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter being investigated is related to the individual’s position at the institution; or
- B) (U//FOUO) The matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

⁷ (U//FOUO) The use of Search Warrants to obtain this information in Preliminary Investigations is prohibited. (See DIOG Section 18.6.8.4.2.3)

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of “academic freedom” (e.g., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a SIM even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

6.11 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements, and FBI field office collection requirements may be collected incidental to a Predicated Investigation. When information that is responsive to these requirements is incidentally collected in a Predicated Investigation, it should be forwarded to the Field Intelligence Group (FIG) for evaluation and potential dissemination against collection requirements. (See DIOG Section 15.6.1.2 - Written Intelligence Products) All incidental collection must be documented in the 8151 field office file.

(U//FOUO) Prior to submitting to the FIG any information that may be evidentiary and therefore potentially discoverable, the FBI employee should discuss with the CDC or OGC the potential impact disseminating the information in an intelligence product may have on the prosecution of the investigation. To the extent dissemination might or is likely to have an adverse impact on the prosecution, the FBI, in consultation with the prosecuting attorney, must assess whether the need for dissemination outweighs the probable impact the dissemination may have on the prosecution.

6.12 (U) STANDARDS FOR APPROVING THE CLOSING OF A PRELIMINARY INVESTIGATION

6.12.1 (U) STANDARDS

(U//FOUO) At the conclusion of a Preliminary Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

- A) (U//FOUO) A summary of the results of the investigation;
- B) (U//FOUO) Whether all logical and reasonable investigation was completed;
- C) (U//FOUO) Whether all investigative methods/techniques initiated have been completed and/or discontinued;
- D) (U//FOUO) Whether all leads set have been completed and/or discontinued;
- E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and
- F) (U//FOUO) A summary statement of the basis on which the Preliminary Investigation will be closed, and a selection of the appropriate closing status:
 - 1) (U//FOUO) C-4: Administrative Closing, which includes:

- a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security
 - b) (U//FOUO) Investigation assigned a new file number
 - c) (U//FOUO) Investigation consolidated into a new file number or an existing file number, or
 - d) (U//FOUO) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted
- 2) (U//FOUO) C-5: USA Declination Closing, which includes:
- a) (U//FOUO) The USAO declined prosecution – individual matter declination
 - b) (U//FOUO) The USAO declined prosecution – blanket declination
- 3) (U//FOUO) C-6: Other Closing, which includes:
- a) (U//FOUO) National security investigation has been completed
 - b) (U//FOUO) Prosecution became non-viable for national security reasons
 - c) (U//FOUO) Any other reason to close

6.12.2 (U) APPROVAL REQUIREMENTS TO CLOSE

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 6.12.1) to ensure it contains the above required information and sufficient details of the investigation on which to base the decision to close the Preliminary Investigation. The closing supervisor must note on the closing document “C,” the closing number 4, 5 or 6 (e.g., C-4, C-5 or C-6) and the closing date. The appropriate closing supervisors are:

- A) (U//FOUO) **Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office requires approval from the SSA. Notification to the FBIHQ operational unit may be required by division PGs.
- B) (U//FOUO) **Opened by FBIHQ:** Closing a Preliminary Investigation opened by FBIHQ requires approval from the UC and notification to any appropriate field office.
- C) (U//FOUO) **SIM Opened by a Field Office:** Closing a Preliminary Investigation opened by a field office involving a SIM requires approval from the SAC, written notification to the FBIHQ operational unit and section and the USAO, if the USAO was notified of the opening.
- D) (U//FOUO) **SIM Opened by FBIHQ:** Closing a Preliminary Investigation opened by FBIHQ involving a SIM requires approval from the SC and written notification to any appropriate field office.

6.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program specific requirements, the FBI employee should consult the relevant division's PG. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

7 (U) FULL INVESTIGATIONS

7.1 (U) OVERVIEW

(U//FOUO) The AGG-Dom authorizes a second level of investigative activity—Predicated Investigations. Predicated Investigations that concern federal crimes or threats to the national security are subdivided into Preliminary Investigations (PI) and Full Investigations (Full). A Full Investigation may be opened if there is an “articulable factual basis” of possible criminal or national threat activity, as discussed in greater detail in Section 7.5, below. There are three types of Full Investigations: (i) single and multi-subject; (ii) Enterprise; and (iii) positive foreign intelligence collection.

7.2 (U) PURPOSE AND SCOPE

(U) A Full Investigation may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

(U) The purposes for conducting Full Investigations include such matters as:

- A) (U) determining whether a federal crime is being planned, prepared for, occurring or has occurred;
- B) (U) identifying, locating, and apprehending the perpetrators;
- C) (U) obtaining evidence for prosecution;
- D) (U) identifying threats to the national security;
- E) (U) investigating an enterprise (as defined in DIOG Section 8); or
- F) (U) collecting positive foreign intelligence (PFI) (as defined in DIOG Section 9).

(U) The investigation of threats to the national security can be investigated under the FBI’s criminal investigation authority or its authority to investigate threats to the national security. As with criminal investigations, detecting and solving crimes, gathering evidence and arresting and prosecuting the perpetrators are frequently the objectives of investigations relating to threats to the national security. These investigations also serve important purposes outside the ambit of normal criminal investigations, however, by providing the basis for decisions concerning other measures needed to protect the national security.

(U//FOUO) A Full Investigation solely for the collection of positive foreign intelligence extends the sphere of the FBI’s information gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States’ foreign affairs. (See DIOG Section 9)

7.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound

judgment and discretion. In order to protect civil liberties in the conduct of criminal and national security investigations, every Full Investigation under this subsection must have adequate predication that is documented in the opening communication.

(U) No investigative activity, including Full Investigations, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors. Full Investigations of individuals, groups or organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the subject. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Full Investigation.

(U) *Example:* Individuals or groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. A Full Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom authorize all lawful investigative methods in the conduct of a Full Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat or the importance of a foreign intelligence requirement.

(U) By emphasizing the use of the least intrusive means to obtain intelligence or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still reasonable based upon the circumstances of the investigation—from the available options to obtain the intelligence, information or evidence. (See DIOG Section 4)

7.4 (U) LEGAL AUTHORITY

7.4.1 (U) CRIMINAL INVESTIGATIONS

(U) The FBI has statutory authority to investigate all federal crime not assigned exclusively to another federal agency. (See 28 U.S.C. § 533; 18 U.S.C. § 3052; 28 C.F.R. § 0.85 [a].)

(U) The FBI also has special investigative jurisdiction to investigate violations of state law in limited circumstances. Specifically, the FBI has jurisdiction to investigate felony killings of state law enforcement officers (28 U.S.C. § 540), violent crimes against interstate travelers (28 U.S.C.

§ 540A), and serial killers (28 U.S.C. § 540B). Authority to investigate these matters is contingent on receiving a request by an appropriate state official.

7.4.2 (U) THREATS TO THE NATIONAL SECURITY

(U) The FBI has authority to investigate threats to the national security pursuant to executive orders, Attorney General authorities, and various statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.)

(U) “Threats to the national security” are specifically defined to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order. (AGG-Dom, Part VII.S)

7.4.3 (U) FOREIGN INTELLIGENCE COLLECTION

(U) The FBI authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note (incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003).

(U) “Foreign Intelligence” is defined as information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists. (AGG-Dom, Part VII.E)

7.5 (U) PREDICATION

(U) A Full Investigation may be opened if there is an “articulable factual basis” that reasonably indicates one of the following circumstances exists:

- A) (U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity;
- B) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat; or
- C) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3, above.

(U//FOUO) Examples: The following examples have sufficient predication to open a Full Investigation:

- A) (U//FOUO) corroborated information from an intelligence agency states that an individual is a member of a terrorist group;

- B) (U//FOUO) an analyst discovers on a blog a threat to a specific home builder and additional information connecting the blogger to a known terrorist group; and
- C) (U//FOUO) FBI DI has posted an authorized PFI requirement for collection.

7.6 (U) STANDARDS FOR OPENING OR APPROVING A FULL INVESTIGATION

(U//FOUO) Before opening or approving the conduct of a Full Investigation, an FBI employee or approving official must determine whether:

- A) (U//FOUO) Adequate predication exist for opening a Full Investigation;
- B) (U//FOUO) The Full Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and
- C) (U//FOUO) The Full Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Full Investigations involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in DIOG Appendix G – Classified Provisions [No Foreign Policy Objection (NFPO)].

(U//FOUO) A Full Investigation cannot be opened solely based on an FBI collection requirement.

7.7 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, NOTICE, PENDING INACTIVE STATUS, FILE REVIEW, AND LETTER HEAD MEMORANDUM

7.7.1 (U) OPENING DOCUMENTATION

(U//FOUO) The predication to open a Full Investigation must be documented in the opening EC. The appropriate approving authority may grant oral authority to open a Full Investigation if the standards for opening or approving a Full Investigation are met. Should oral authorization to conduct a Full Investigation be granted, an EC setting forth the predicated facts, as well as the identity of the authorizing supervisor and date of oral authorization, must be documented to the supervisor who granted the oral authorization, as soon as practicable, but not more than five (5) business days after granting the authorization.

(U//FOUO) If at the time of the opening, or at anytime thereafter, the Full Investigation involves a sensitive investigative matter, the title/caption must contain the words “Sensitive Investigative Matter.”

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. See DIOG Appendix J.

7.7.1.1 (U) APPROVAL / EFFECTIVE DATE / NOTICE

(U//FOUO) The effective date of the Full Investigation is the date the final approval authority (e.g., SSA or SAC) approves the EC by electronic signature/date generated by Sentinel or by handwriting their initials and date on the EC. If the Full Investigation is opened on oral

authority, the date on which the oral authority was granted is the date the investigation was opened. See Section 3.4.2.2.

- A) (U//FOUO) **Opened By a Field Office:** The opening of a Full Investigation for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) by a field office requires prior approval of the SSA with written notification within 15 calendar days of the opening to the responsible FBIHQ operational unit. The opening of a Full Investigation of a United States person (USPER) relating to a threat to the national security for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires the responsible FBIHQ-NSB unit to notify DOJ NSD as soon as practicable, but in all events within 30 calendar days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to DOJ NSD also apply.
- B) (U//FOUO) **Opened By FBIHQ:** The opening of a Full Investigation by FBIHQ for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) requires prior approval of the UC with written notification within 15 calendar days of the opening to any appropriate field office. The opening of a Full Investigation by FBIHQ of an USPER relating to a threat to the national security for circumstances described in Sections 7.5.A and 7.5.B (i.e., for any reason other than to collect intelligence that is responsive to a PFI requirement) also requires notice to DOJ NSD as soon as practicable, but in all events within 30 days after the investigation is opened or the subject is determined to be an USPER. If the subject of the investigation is a non-USPER and later becomes or is determined to be an USPER, the notice provisions in this subsection to the field office and DOJ also apply.
- C) (U//FOUO) **Sensitive Investigative Matters (SIM):** The opening of a Full Investigation involving a sensitive investigative matter:
- 1) (U//FOUO) **SIM Opened By a Field Office:** requires prior CDC review and SAC approval, and written notification (EC and disseminable LHM) to the appropriate FBIHQ operational UC and SC within 15 calendar days following the opening. Additionally, the field office must notify the USAO, in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the United States Attorney (USA)), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division official or NSD official as soon as practicable, but no later than 30 calendar days after the investigation is opened. The notice must identify all known sensitive investigative matters involved in the investigation (see DIOG Appendix G – Classified Provisions for additional notice requirements). If a sensitive investigative matter arises after the opening of a Full Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be furnished as specified above.
 - 2) (U//FOUO) **SIM Opened By FBIHQ:** requires prior OGC review and SC approval, and written notification (EC and disseminable LHM) to any appropriate field office within 15 calendar days following the opening. Additionally, FBIHQ operational unit must notify the

appropriate USAO(s) in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the USA) or the matter is a counterintelligence or espionage investigation; and the appropriate DOJ Criminal Division official or NSD official, as soon as practicable, but no later than 30 calendar days after such an investigation is opened. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the “circumstances” exception described above, FBIHQ must explain the circumstances in the written notice to the field office(s) and DOJ. The notice must identify all known sensitive investigative matters involved in the investigation (see DIOG Appendix G - Classified Provisions for additional notice requirements). If a sensitive investigative matter arises after the opening of a Full Investigation, investigative activity may continue, but the matter must be reviewed by OGC and approved by the appropriate FBIHQ SC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be furnished as specified above. (AGG-Dom, Part II.B.5.a)

- D) (U//FOUO) ***Positive Foreign Intelligence Full Investigation:*** The opening of a Full Investigation in order to collect positive foreign intelligence for circumstances described in Section 7.5.C above must be approved as provided in DIOG Section 9. Additionally, written notification to FBIHQ Domain, Collection, HUMINT Management Section (DCHMS) SC and DOJ NSD is required as soon as practicable but no later than 30 calendar days after opening the investigation.
- E) (U//FOUO) ***FBIHQ Disapproves Opening:*** The EAD for the National Security Branch (NSB) must notify the Deputy Attorney General if FBIHQ disapproves a field office’s opening of a Full Investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient, and the EAD for the NSB is responsible for establishing a system that will allow for the prompt retrieval of such denials. (AGG-Dom, Part II.B.5.d)

7.7.2 (U) PENDING INACTIVE STATUS

(U//FOUO) A Full Investigation may be placed in “pending inactive” status once all logical investigation has been completed and only prosecutive action or other disposition remains to be reported. Examples of Full Investigations that may be placed in “pending inactive” status would include, but not be limited to: criminal investigations pending an appeal; fugitive investigations, when all logical investigation has been conducted and the subject is still in fugitive status; parental kidnapping investigations, when the parent who kidnapped the child is residing in a foreign country and the local authorities will not or cannot extradite the subject back to the United States.

7.7.3 (U) FILE REVIEW

(U//FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary FBI employees must be conducted at least every 60 days.

7.7.4 (U) ANNUAL LETTERHEAD MEMORANDUM

(U//FOUO) Annual letterhead memoranda regarding the status of Full Investigations are not required by the AGG-Dom; however, the FBIHQ operational divisions may require such reports

in their PGs. See foreign intelligence collection in Section 9 for annual reporting requirements to FBIHQ DCHMS and DOJ.

7.8 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN FULL INVESTIGATIONS

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee or approving official must determine whether:

- A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;
- B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation;
- C) (U//FOUO) If the Full Investigation is for collecting positive foreign intelligence, the FBI is operating openly and consensually with a USPER, to the extent practicable; and
- D) (U//FOUO) The method to be used is an appropriate use of personnel and financial resources.

7.9 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) All lawful methods may be used in a Full Investigation, unless the investigation is to collect foreign intelligence. A complete discussion of these investigative methods, including approval requirements, is contained in [Section 18](#). The use or dissemination of information obtained by the use of these methods must comply with the AGG-Dom and DIOG Section 14. The following investigative methods are authorized to be used in all Full Investigations, other than investigations to collect foreign intelligence:

- A) (U) Public information. (Section [18.5.1](#))
- B) (U) Records or information - FBI and DOJ. (Section [18.5.2](#))
- C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section [18.5.3](#))
- D) (U) On-line services and resources. (Section [18.5.4](#))
- E) (U) CHS use and recruitment. (Section [18.5.5](#))
- F) (U) Interview or request information from the public or private entities. (Section [18.5.6](#))
- G) (U) Information voluntarily provided by governmental or private entities. (Section [18.5.7](#))
- H) (U) Physical Surveillance (not requiring a court order). (Section [18.5.8](#))
- I) (U) Consensual monitoring of communications, including electronic communications. (Section [18.6.1](#))

(U//FOUO) *Note:* For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an Otherwise Illegal Activity (OIA). Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an Assistant Special Agent-in-Charge (ASAC) or Supervisory Special Agent (SSA).

- (U//FOUO) See the classified provisions in Appendix G for additional information.
- J) (U) Intercepting the communications of a computer trespasser. (Section 18.6.2)
 - K) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
 - L) (U) Administrative subpoenas. (Section 18.6.4)
 - M)(U) Grand jury subpoenas. (Section 18.6.5)
 - N) (U) National Security Letters. (Section 18.6.6)
 - O) (U) FISA Order for business records. (Section 18.6.7).
 - P) (U) Stored wire and electronic communications and transactional records. (Section 18.6.8)
 - Q) (U) Pen registers and trap/trace devices. (Section 18.6.9)
 - R) (U) Mail covers. (Section 18.6.10)
 - S) (U) Polygraph examinations. (Section 18.6.11)
 - T) (U) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)
 - U) (U) Undercover Operations (Section 18.6.13)
 - V) (U) Searches – with a warrant or court order. (Section 18.7.1)
 - W)(U) Electronic surveillance – Title III. (Section 18.7.2)
 - X) (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (Section 18.7.3)
- (U) See the classified provisions in DIOG Appendix G for additional information.

7.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN FULL INVESTIGATIONS

(U//FOUO) The title/caption of the opening or subsequent EC for a Full Investigation involving a sensitive investigative matter must contain the words “Sensitive Investigative Matter.” DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve a Full Investigation involving a SIM.

7.10.1 (U) SIM CATEGORIES IN FULL INVESTIGATIONS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, news media, and academic nexus.

7.10.2 (U) ACADEMIC NEXUS IN FULL INVESTIGATIONS

(U//FOUO) As a matter of FBI policy, an investigative activity having an “academic nexus” is considered a SIM if:

- A) (U//FOUO) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under a Predicated Investigation is related to the individual’s position at the institution; or
- B) (U//FOUO) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of “academic freedom” (i.e., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a sensitive investigative matter even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

7.11 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements, and FBI field office collection requirements may be collected incidental to a Predicated Investigation. When information that is responsive to these requirements is incidentally collected in a Predicated Investigation, it should be forwarded to the FIG for evaluation and potential dissemination against collection requirements <http://home.fbinet.fbi/forms/fd1028/DIOG/Lists/Program Policy Guides/AllItems.aspx>. (See DIOG Section 15.6.1.2 - Written Intelligence Products) All incidental collection must be documented in the 815I field office file.

(U//FOUO) Prior to submitting to the FIG any information that may be evidentiary and therefore potentially discoverable, the FBI employee should discuss with the CDC or OGC the potential impact disseminating the information in an intelligence product may have on the prosecution of the investigation. To the extent dissemination might or is likely to have an adverse impact on the prosecution, the FBI, in consultation with the prosecuting attorney, must assess whether the need for dissemination outweighs the probable impact the dissemination may have on the prosecution.

(U) Because the authority to collect positive foreign intelligence enables the FBI to obtain information pertinent to the United States’ conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information gathered may concern lawful activities. Accordingly, the FBI must operate openly and consensually with an USPER to the extent practicable when collecting positive foreign intelligence that does not concern criminal activities or threats to the national security.

7.12 (U) STANDARDS FOR APPROVING THE CLOSING OF A FULL INVESTIGATION**7.12.1 (U) STANDARDS**

(U//FOUO) At the conclusion of a Full Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

- A) (U//FOUO) A summary of the results of the investigation;
- B) (U//FOUO) Whether sufficient personnel and financial resources were expended on the investigation, or an explanation/justification for not expending sufficient resources;
- C) (U//FOUO) Whether logical and reasonable investigation was completed;
- D) (U//FOUO) Whether all investigative methods/techniques initiated have been completed and/or discontinued;
- E) (U//FOUO) Whether all leads set have been completed and/or discontinued;
- F) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and
- G) (U//FOUO) A summary statement of the reason the Full Investigation will be closed, and selection of the appropriate closing status:
 - 1) (U//FOUO) C-4: Administrative Closing, which includes:
 - a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security
 - b) (U//FOUO) Investigation assigned a new file number
 - c) (U//FOUO) Investigation consolidated into a new file number or an existing file number
 - d) (U//FOUO) Unaddressed Work investigation file closed because no investigation or no further investigation will be conducted
 - 2) (U//FOUO) C-5: USA Declination Closing, which includes:
 - a) (U//FOUO) The USAO declined prosecution – individual matter declination
 - b) (U//FOUO) The USAO declined prosecution – blanket declination
 - 3) (U//FOUO) C-6: Other Closing, which includes:
 - a) (U//FOUO) Final prosecution or final prosecutive action has been completed
 - b) (U//FOUO) National security investigation has been completed
 - c) (U//FOUO) Prosecution became non-viable for national security reasons
 - d) (U//FOUO) A federal grand jury returned a “No True Bill”
 - e) (U//FOUO) A nolle prosequi has been entered with the court
 - f) (U//FOUO) any other reason for closing

7.12.2 (U) APPROVAL REQUIREMENTS TO CLOSE

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 7.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Full Investigation. The closing supervisor must note on the closing document “C,” the closing number 4, 5 or 6 (e.g., C-4, C-5 or C-6) and the closing date. Although there is no duration limit for a Full Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

- A) (U//FOUO) Opened by a Field Office: Closing a Full Investigation opened by a field office requires approval from the SSA. Notification to the FBIHQ operational unit may be required by division PGs.
- B) (U//FOUO) Opened by FBIHQ: Closing a Full Investigation opened by FBIHQ requires approval from the UC and notification to the appropriate field office.
- C) (U//FOUO) SIM Opened by a Field Office: Closing a Full Investigation opened by a field office involving a sensitive investigative matter requires approval from the SAC and written notification to the FBIHQ operational unit and section and the USAO, if the USAO was notified of the opening.
- D) (U//FOUO) SIM Opened by FBIHQ: Closing a Full Investigation opened by FBIHQ involving a sensitive investigative matter requires approval from the SC and written notification to the appropriate field office.
- E) (U//FOUO) Positive Foreign Intelligence: (See DIOG Section 9)

7.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division’s PG to ascertain any program-specific requirements. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

8 (U) ENTERPRISE INVESTIGATIONS (EI)

8.1 (U) OVERVIEW

(U) An Enterprise Investigation (EI) may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation as described in DIOG Section 7, although there are additional approval requirements that affect Enterprise Investigations. An Enterprise Investigation focuses on a group or organization that may be involved in the most serious criminal or national security threats to the public, as described in Section 8.5 below. An Enterprise Investigation cannot be conducted as Preliminary Investigation or an Assessment, nor may they be conducted for the sole purpose of collecting positive foreign intelligence (PFI). See Section 8.2, below, regarding Preliminary Investigations and Assessments.

8.2 (U) PURPOSE, SCOPE AND DEFINITIONS

(U) **Enterprise defined:** An enterprise is a group of persons associated together for a common purpose of engaging in a course of conduct. The term “enterprise” includes any partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact, although not a legal entity.

(U) **Associated in fact defined:** The term “associated in fact” means the persons have an ongoing organization, formal or informal, and that the persons function together as a continuing unit.

(U) **Purpose/Scope:** The purpose of an Enterprise Investigation is to examine the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (Attorney General’s Guidelines for Domestic FBI Operations (AGG-Dom), Part II.C.2)

(U) **Note:** Enterprise Investigations were designed, among other things, to combine and replace the traditional “Racketeering Enterprise Investigations” (92 classification) and “Terrorism Enterprise Investigations” (100 classification). An Enterprise Investigation is only authorized to be opened on the most serious criminal or national security threats. The term Enterprise Investigation as used in the DIOG should not be confused with other usages of the word “enterprise,” such as criminal enterprise investigations (e.g., 281 classification, 245 classification, etc.), which are not Enterprise Investigations as defined in DIOG Section 8. See DIOG Sections 8.4 and 8.5.

(U//FOUO) Although an Enterprise Investigation may not be conducted as a Preliminary Investigation, a Preliminary Investigation may be used to determine whether a group or organization is a criminal or terrorist enterprise if the FBI has “information or an allegation” that an activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur, and the investigation may obtain

information relating to the activity of the group or organization in such activity. An Assessment may also be opened to determine whether a group or organization is involved in activities constituting violations of federal criminal law or threats to the national security.

8.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion. In order to protect civil liberties in the conduct of criminal and national security investigations, every Full Investigation, including an Enterprise Investigation under this subsection, must have adequate predication documented in the opening communication.

(U) No investigative activity, including an Enterprise Investigation, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject or a combination of only those factors. An Enterprise Investigation of groups and organizations must focus on activities related to the threats or crimes being investigated, not solely on First Amendment activities or on the race, ethnicity, national origin or religion of the members of the group or organization. In this context, it is particularly important clearly to identify and document the law enforcement or national security basis of the Enterprise Investigation.

(U//FOUO) *Example:* Groups who communicate with each other or with members of the public in any form in pursuit of social or political causes—such as opposing war or foreign policy, protesting government actions, promoting certain religious beliefs, championing particular local, national, or international causes, or a change in government through non-criminal means, and actively recruit others to join their causes—have a fundamental constitutional right to do so. An Enterprise Investigation may not be opened based solely on the exercise of these First Amendment rights.

(U) The AGG-Dom authorizes all lawful investigative methods in the conduct of an Enterprise Investigation. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. A more intrusive method may be warranted in light of the seriousness of a criminal or national security threat.

(U) By emphasizing the use of the least intrusive means to obtain information, intelligence and/or evidence, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the investigation, including targets, witnesses, and victims. This principle is not intended to discourage FBI employees from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage FBI employees to choose the least intrusive—but still effective means—from the available options to obtain the information, intelligence or evidence. See DIOG Section 4.4.

8.4 (U) PREDICATION

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for: (AGG-Dom, Part II.C.1)

A) (U) **Racketeering Activity:**

(U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5) - (92 and 305A matters may be opened as Enterprise Investigations-Racketeering Activity (EI/RA));

B) (U) **International Terrorism:**

(U) International terrorism, as defined in 18 U.S.C. § 2331 and AGG-Dom, Part VII.J or other national security threat – (415 matters may be opened as Enterprise Investigations);

C) (U) **Domestic Terrorism:**

- 1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law - (100 matters may be opened as Enterprise Investigations);
- 2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law – (100 matters may be opened as Enterprise Investigations); or
- 3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43 – (100 matters may be opened as Enterprise Investigations).

(U) The “articulable factual basis” for opening an Enterprise Investigation is met with the identification of a group whose statements made in furtherance of its objectives or its conduct demonstrate a purpose of committing crimes or securing the commission of crimes by others. The group’s activities and statements of its members may be considered in combination to comprise the “articulable factual basis,” even if the statements alone or activities alone would not warrant such a determination.

(U//FOUO) **Examples:** The following examples demonstrate sufficient predication to open an Enterprise Investigation:

- A) (U//FOUO) The “North Eucre Liberation Army” declares its intent to obtain dangerous biological agents in the United States to support its fight against the South Eucre Liberation Army, even though the FBI has no evidence that it has acquired anything.
- B) (U//FOUO) Organized crime family members extort a number of contractors in a particular industry for illicit economic gain.
- C) (U//FOUO) A group known as “Basket of Cuddly Puppies” harshly denounces puppy mills, and several puppy mills become the victim of arson, shortly after which internet postings appear on the group’s website stating, “Now, maybe they’ll take us seriously.” If there were only a harsh denouncement and no link to the crimes, this would not constitute predication for an Enterprise Investigation because the only fact known about the group would be its denouncement of puppy mills—an action protected by the First Amendment.

8.5 (U) STANDARDS FOR OPENING OR APPROVING AN ENTERPRISE INVESTIGATION

(U//FOUO) Before opening or approving the conduct of an Enterprise Investigation, an FBI employee or approving official must determine whether:

- A) (U//FOUO) Adequate predication exists for opening an Enterprise Investigation;
- B) (U//FOUO) The Enterprise Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and
- C) (U//FOUO) The Enterprise Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Enterprise Investigation involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as subjects may be found in DIOG Appendix G – Classified Provisions [No Foreign Policy Objection (NFPO)].

(U//FOUO) A Predicated Investigation, including an Enterprise Investigation, cannot be opened solely based on an FBI collection requirement.

8.6 (U) OPENING DOCUMENTATION, EFFECTIVE DATE, APPROVAL, NOTICE, AND FILE REVIEW**8.6.1 (U) OPENING DOCUMENTATION**

(U//FOUO) The predication to open an Enterprise Investigation must be documented in the opening electronic communication (EC).

(U//FOUO) If at the time of the opening, or at anytime thereafter, the Enterprise Investigation (EI) involves a sensitive investigative matter (SIM), the title/caption must contain the words “Sensitive Investigative Matter.”

(U//FOUO) The appropriate approving authority (Section Chief) may grant oral authority to open an Enterprise Investigation if the standards for opening or approving an Enterprise Investigation are met. Should oral authorization to conduct an Enterprise Investigation be granted, an EC setting forth the predicated facts, as well as the identity of the approving official(s) (i.e., SC), and the date of oral authorization must be documented to the approving official(s) who granted the oral authorization as soon as practicable, but not more than five (5) business days after granting oral authorization.

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

8.6.2 (U) EFFECTIVE DATE

(U//FOUO) The effective date of the Enterprise Investigation is the date the final approval authority (i.e., SC) approves the EC by electronic signature/date generated by Sentinel or by handwriting their initials and date on the EC. If the Enterprise Investigation is opened on oral

authority, the date on which the oral approval authority was granted is the effective date. See DIOG Section 3.4.2.2.

8.6.3 (U) APPROVAL REQUIREMENTS FOR OPENING AN ENTERPRISE INVESTIGATION

8.6.3.1 (U) EI OPENED BY A FIELD OFFICE WITH SECTION CHIEF APPROVAL

(U//FOUO) The opening of an Enterprise Investigation by an FBI field office requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the United States Attorney's Office (USAO) and the Department of Justice (DOJ) as specified below.

8.6.3.2 (U) EI OPENED BY FBIHQ WITH SECTION CHIEF APPROVAL

(U//FOUO) The opening of an Enterprise Investigation by an FBIHQ division requires the prior approval of the appropriate FBIHQ SC, as well as written notification to the appropriate field office(s), USAO and DOJ as specified below

8.6.3.3 (U) SIM EI OPENED BY A FIELD OFFICE WITH SPECIAL AGENT IN CHARGE AND SECTION CHIEF APPROVAL

(U//FOUO) A SIM Enterprise Investigation opened by a field office requires prior CDC review, SAC and appropriate FBIHQ SC approval, and written notification to DOJ in the form of an LHM or similar documentation. The LHM or similar documentation for dissemination to DOJ must be submitted to the appropriate FBIHQ operational section within 15 calendar days following the opening. Additionally, the field office must notify the USAO, in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption Enterprise Investigation of a group that is personally close to the United States Attorney (USA)), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ operational section must notify, in writing, the appropriate DOJ Criminal Division or National Security Division (NSD) official as soon as practicable, but no later than 30 calendar days after the investigation is opened. The notice must identify all known sensitive investigative matters (SIM) involved in the Enterprise Investigation (see DIOG Appendix G – Classified Provisions for additional notice requirements).

(U//FOUO) If a SIM arises after the opening of an Enterprise Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC and appropriate FBIHQ SC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be furnished as specified above.

8.6.3.4 (U) SIM EI OPENED BY FBIHQ WITH SECTION CHIEF APPROVAL

(U//FOUO) A SIM Enterprise Investigation opened by FBIHQ requires prior OGC review and SC approval, and written notification to DOJ and appropriate field office(s) in the form of an LHM or similar documentation. The LHM or similar documentation for dissemination to the field office(s) must be submitted within 15 calendar days following the opening.

Additionally, the FBIHQ operational unit must notify the appropriate USAO(s) in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption Enterprise Investigation of a group that is personally close to the USA), or the matter is a counterintelligence or espionage investigation. (See CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the FBIHQ operational unit must explain those circumstances in the written notice to the field office(s) and DOJ. The responsible FBIHQ operational section must notify, in writing, the appropriate DOJ Criminal Division or National Security Division (NSD) official as soon as practicable, but no later than 30 calendar days after the investigation is opened. The notice must identify all known sensitive investigative matters (SIM) involved in the Enterprise Investigation (see DIOG Appendix G – Classified Provisions for additional notice requirements).

(U//FOUO) If a SIM arises after the opening of an Enterprise Investigation, investigative activity may continue, but the matter must be reviewed by OGC and approved by the appropriate FBIHQ SC as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be furnished as specified above.

8.6.4 (U) NOTICE REQUIREMENTS

(U//FOUO) FBIHQ division PGs may require specific facts to be included in a field office request to open an Enterprise Investigation. At a minimum, the request must include whether the Enterprise Investigation is a SIM.

(U//FOUO) The responsible FBIHQ section must notify the DOJ NSD or the Organized Crime and Racketeering Section (OCRS) of the opening of an Enterprise Investigation by a field office or by FBIHQ, as soon as practicable but no later than 30 calendar days after the opening of the investigation.

(U//FOUO) For Enterprise Investigations that involve groups of persons who pose a national security threat, the responsible DOJ component for the purpose of notification and reports is the NSD. For Enterprise Investigations relating to a pattern of racketeering activity that does not involve a national security threat, the responsible DOJ component is the OCRS of the Criminal Division. (AGG-Dom, Part II.C.3)

(U) The Assistant Attorney General for National Security or the Chief of the OCRS, as appropriate, may at any time request the FBI to provide a report on the status of an Enterprise Investigation, and the FBI will provide such reports as requested. (AGG-Dom, Part II C.3.d)

8.6.5 (U) FILE REVIEW

(U//FOUO) Supervisory file reviews must be conducted at least once every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary agents must be conducted at least once every 60 days.

8.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN AN ENTERPRISE INVESTIGATION

(U//FOUO) An Enterprise Investigation may only be opened and operated as a Full Investigation and is subject to the same requirements that apply to a Full Investigation. Therefore, the standards for opening or approving the use of investigative methods and the availability of investigative methods that may be used in an Enterprise Investigation are the same as set forth in Sections 7.8 and 7.9.

8.8 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN ENTERPRISE INVESTIGATIONS

(U//FOUO) The title/caption of the opening or subsequent EC for a Full Enterprise Investigation involving a sensitive investigative matter must contain the words “Sensitive Investigative Matter.” DIOG Section 10 contains the required approval authority and factors to be considered when determining whether to conduct or approve a Full Enterprise Investigation involving a SIM.

8.8.1 (U) SIM CATEGORIES IN ENTERPRISE INVESTIGATIONS

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N). As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the DIOG Appendix G – Classified Provisions define domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, news media, and academic nexus.

8.8.2 (U) ACADEMIC NEXUS IN ENTERPRISE INVESTIGATIONS

(U//FOUO) As a matter of FBI policy, an investigative activity having an “academic nexus” is considered a SIM if:

- A) (U//FOUO) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under a Predicated Investigation is related to the individual’s position at the institution; or
- B) (U//FOUO) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of “academic freedom” (e.g., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a sensitive investigative matter even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

8.9 (U) INTELLIGENCE COLLECTION (I.E., INCIDENTAL COLLECTION)

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements and FBI field office collection requirements may be collected incidental to an Enterprise Investigation. When information that is responsive to these requirements is incidentally collected during an Enterprise Investigation, it should be forwarded to the Field Intelligence Group (FIG) for evaluation and potential dissemination against collection requirements. (See DIOG Section 15.6.1.2 - Written Intelligence Products) All incidental collection must be documented in the 8151 field office file.

(U//FOUO) Prior to submitting to the FIG any information that may be evidentiary and therefore potentially discoverable, the FBI employee should discuss with the CDC or OGC the potential impact disseminating the information in an intelligence product may have on the prosecution of the investigation. To the extent dissemination might or is likely to have an adverse impact on the prosecution, the FBI, in consultation with the prosecuting attorney, must assess whether the need for dissemination outweighs the probable impact the dissemination may have on the prosecution.

8.10 (U) STANDARDS FOR APPROVING THE CLOSING OF AN ENTERPRISE INVESTIGATION

8.10.1 (U) STANDARDS

(U//FOUO) At the conclusion of an Enterprise Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

- A) (U//FOUO) A summary of the results of the investigation;
- B) (U//FOUO) Whether logical and reasonable investigation was completed;
- C) (U//FOUO) Whether all investigative methods initiated have been completed and/or discontinued;
- D) (U//FOUO) Whether all leads set have been completed and/or discontinued;
- E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and
- F) (U//FOUO) A summary statement of the basis on which the Enterprise Investigation will be closed, and selection of the appropriate closing status:
 - 1) (U//FOUO) C-4: Administrative Closing, which includes:
 - a) (U//FOUO) No further investigation is warranted because logical investigation and/or leads have been exhausted, and the investigation to date did not identify a criminal violation or a priority threat to the national security
 - b) (U//FOUO) Investigation assigned a new file number, or
 - c) (U//FOUO) Investigation consolidated into a new file number or an existing file number.

- 2) (U//FOUO) C-6: Other Closing, which includes:
- a) (U//FOUO) Enterprise Investigation has been completed; or
 - b) (U//FOUO) Any other type of closing

8.10.2 (U) APPROVAL REQUIREMENTS TO CLOSE

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 8.10.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base the decision to close the Enterprise Investigation. The closing supervisor must note on the closing document "C," the closing status using 4 or 6 (e.g., C-4 or C-6) and the closing date. Although there is no limit on the duration of an Enterprise Investigation, the investigation must be closed upon all investigative activity being exhausted. The appropriate closing supervisors are:

- A) (U//FOUO) **Opened by a Field Office with FBIHQ SC Approval:** Closing an Enterprise Investigation opened by a field office requires the prior approval of the appropriate FBIHQ SC.
 - B) (U//FOUO) **Opened by FBIHQ:** Closing an Enterprise Investigation opened by FBIHQ requires approval from the appropriate SC and notification to the appropriate field office.
 - C) (U//FOUO) **SIM Opened by a Field Office with FBIHQ SC Approval:** Closing an Enterprise Investigation opened by a field office involving a sensitive investigative matter requires approval from the appropriate FBIHQ SC.
- (U//FOUO) **SIM Opened by FBIHQ:** Closing an Enterprise Investigation opened by FBIHQ involving a sensitive investigative matter requires approval from the SC, and written notification to the appropriate field office.

8.11 (U) OTHER PROGRAM SPECIFIC INVESTIGATIVE REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements. FBIHQ division PGs, however, may not contradict, alter or otherwise modify the standards established in the DIOG.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

This Page is Intentionally Blank.

9 (U) FOREIGN INTELLIGENCE

9.1 (U) OVERVIEW

(U) **Foreign Intelligence defined:** Foreign intelligence is “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists.” A “Foreign Intelligence Requirement” is a collection requirement issued under the authority of the Director of National Intelligence (DNI) and accepted by the FBI Directorate of Intelligence (DI). Additionally, the President, a United States Intelligence Community (USIC) office designated by the President, the Attorney General, Deputy Attorney General, or other designated Department of Justice (DOJ) official may levy a foreign intelligence requirement on the FBI. Foreign intelligence collection by the FBI is based upon requirements.

(U//FOUO) Foreign intelligence requirements issued by one of the parties listed above and accepted by the FBI DI will fall into one of two categories: (i) those that address national security issues that are within the FBI’s core national security mission (FBI collection requirements); and (ii) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists which are not within the FBI’s core national security mission (PFI Collection Requirements).

(U//FOUO) Requirements which fall into the first category may correspond to FBI national collection requirements as defined in DIOG Section 5.12. FBI national collection requirements are addressed in properly authorized Assessments (See DIOG Section 5.6.3.5) or Predicated Investigations. (See the Intelligence Policy Implementation Guide (IPG) for specific requirements.)

(U//FOUO) Requirements which fall into the second category are known as Positive Foreign Intelligence (PFI) Collection Requirements and may only be addressed under the authorities described in this section. Type 6 Assessments opened for the purpose of determining whether a field office has the ability to collect on a PFI Collection Requirement (See DIOG Section 5.6.3.5), and Full Investigations opened for the specific purpose of collecting on PFI Collection Requirements must be predicated on an established PFI Collection Requirement that has been accepted and approved by the FBIHQ Directorate of Intelligence (DI) – Domain Collection and HUMINT Management Section (DCHMS), Domain Collection Program Management Unit (DCPMU) UC. Preliminary Investigations for the sole purpose of collecting on PFI requirements are not authorized by the AGG-Dom. A Full PFI Investigation to collect on PFI Collection Requirements must be opened in the 809-814 or 816 classification files. A Full PFI Investigation opened for the intended purpose of collecting on PFI requirements must be approved by the DCPMU Unit Chief (UC). A Full PFI Investigation cannot be opened on oral authority.

(U//FOUO) “The general guidance of the FBI’s foreign intelligence collection activities by DNI-authorized requirements does not limit the FBI’s authority to conduct investigations supportable on the basis of its other authorities—to investigate federal crimes and threats to the national security—in areas in which the information sought also falls under the definition of foreign

9 (U) FOREIGN INTELLIGENCE

9.1 (U) OVERVIEW

(U) **Foreign Intelligence defined:** Foreign intelligence is “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists.” A “Foreign Intelligence Requirement” is a collection requirement issued under the authority of the Director of National Intelligence (DNI) and accepted by the FBI Directorate of Intelligence (DI). Additionally, the President, a United States Intelligence Community (USIC) office designated by the President, the Attorney General, Deputy Attorney General, or other designated Department of Justice (DOJ) official may levy a foreign intelligence requirement on the FBI. Foreign intelligence collection by the FBI is based upon requirements.

(U//FOUO) Foreign intelligence requirements issued by one of the parties listed above and accepted by the FBI DI will fall into one of two categories: (i) those that address national security issues that are within the FBI’s core national security mission (FBI collection requirements); and (ii) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists which are not within the FBI’s core national security mission (PFI Collection Requirements).

(U//FOUO) Requirements which fall into the first category may correspond to FBI national collection requirements as defined in DIOG Section 5.12. FBI national collection requirements are addressed in properly authorized Assessments (See DIOG Section 5.6.3.5) or Predicated Investigations. (See the Intelligence Policy Implementation Guide (IPG) for specific requirements.)

(U//FOUO) Requirements which fall into the second category are known as Positive Foreign Intelligence (PFI) Collection Requirements and may only be addressed under the authorities described in this section. Type 6 Assessments opened for the purpose of determining whether a field office has the ability to collect on a PFI Collection Requirement (See DIOG Section 5.6.3.5), and Full Investigations opened for the specific purpose of collecting on PFI Collection Requirements must be predicated on an established PFI Collection Requirement that has been accepted and approved by the FBIHQ Directorate of Intelligence (DI) – Domain Collection and HUMINT Management Section (DCHMS), Domain Collection Program Management Unit (DCPMU) UC. Preliminary Investigations for the sole purpose of collecting on PFI requirements are not authorized by the AGG-Dom. A Full PFI Investigation to collect on PFI Collection Requirements must be opened in the 809-814 or 816 classification files. A Full PFI Investigation opened for the intended purpose of collecting on PFI requirements must be approved by the DCPMU Unit Chief (UC). A Full PFI Investigation cannot be opened on oral authority.

(U//FOUO) “The general guidance of the FBI’s foreign intelligence collection activities by DNI-authorized requirements does not limit the FBI’s authority to conduct investigations supportable on the basis of its other authorities—to investigate federal crimes and threats to the national security—in areas in which the information sought also falls under the definition of foreign

intelligence.” (Attorney General’s Guidelines for Domestic FBI Operations (AGG-Dom), Introduction A.3) Accordingly, the AGG-Dom authorizes the collection of foreign intelligence incidental to predicated criminal, counterintelligence, counterterrorism, cyber, and weapons of mass destruction investigations. Incidental collection described above must be documented in the 815I field office classification file. See DIOG Sections 5.2 and 7.5.A and B.

(U//FOUO) A Full PFI Investigation can be opened based solely on a PFI Collection Requirement. The authorized purpose (the PFI Collection requirement) must exist and have been accepted by the FBI.

(U) *Examples:*

- A) (U//FOUO) The USIC seeks information regarding the intentions of the Republic of X to strengthen its military in the wake of hostile actions by the Government of Y. If FBIHQ DI accepts this requirement as a PFI Collection Requirement, FBIHQ DI will approve a file in the 809-814 or 816 investigative classification series. Any field office which has the capacity to respond to this requirement must operate under the 809-814 or 816 series file. This may be opened as a Full Investigation if authorized by DCPMU.
- B) (U//FOUO) The USIC seeks information regarding the Government of Y’s intentions vis-à-vis the Republic of X. FBIHQ DI accepts this requirement as a PFI Collection Requirement and approves the opening of a file in the 809-814 or 816 investigative classification series. As part of an existing counterintelligence investigation, an operational squad has technical coverage that is yielding information pertinent to this requirement. The operational squad should share relevant foreign intelligence collected during the course of its investigation with the Field Intelligence Group (FIG), which should analyze and disseminate that foreign intelligence information and document its handling of the intelligence in the appropriate 809-814 or 816 classification file.

(U//FOUO) FBIHQ DI provides specific guidance in its IPG regarding FBI national collection requirements, FBI field office collection requirements, and PFI requirements.

9.2 (U) PURPOSE AND SCOPE

(U//FOUO) As stated above, foreign intelligence is “information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists.” The collection of positive foreign intelligence extends the sphere of the FBI’s information-gathering activities beyond federal crimes and threats to the national security and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States’ foreign affairs. (AGG-Dom, Introduction A.3)

(U//FOUO) While employees may collect positive foreign intelligence in already opened Assessments and Predicated Investigations (incidental collection), this section is focused on the policies and procedures that govern opening and managing Full Investigations for the specific purpose of collecting on PFI Collection Requirements published by the DI. DIOG Section 5.6.3.4 governs opening and managing Type 6 Assessments.

9.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) Because the authority to collect positive foreign intelligence pursuant to PFI Collection Requirements enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information collected may concern lawful activities. Accordingly, **the FBI must operate openly and consensually with an US Person (USPER)**, to the extent practicable, when collecting positive foreign intelligence. (AGG-Dom, Introduction A.3)

(U) The pursuit of legitimate investigative goals without infringing upon the exercise of constitutional freedoms is a challenge that the FBI meets through the application of sound judgment and discretion.

(U) No investigative activity, including the collection of positive foreign intelligence pursuant to PFI Collection Requirements, may be taken solely on the basis of activities that are protected by the First Amendment or on the race, ethnicity, national origin or religion of the subject or a combination of only those factors. In order to take action intentionally to collect positive foreign intelligence, an FBI employee must open a Full Investigation that is predicated on a PFI requirement.

(U) The AGG-Dom present investigators with a number of authorized investigative methods in the conduct of a Full Investigation to collect positive foreign intelligence. Considering the effect on the privacy and civil liberties of individuals and the potential to damage the reputation of individuals, some of these investigative methods are more intrusive than others. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used, but the FBI must not hesitate to use any lawful method consistent with the AGG-Dom. For further explanation of the least intrusive method refer to DIOG Section 4.

(U) Moreover, when collecting positive foreign intelligence, as part of a Full Investigation predicated on a PFI requirement, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U) By emphasizing the use of the least intrusive means to collect positive foreign intelligence and by emphasizing the need to operate openly and consensually with an USPER, to the extent practicable, FBI employees can effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encountered as part of the collection. This principle is not intended to discourage FBI employees from seeking relevant and necessary positive foreign intelligence, but rather is intended to make sure FBI employees choose the least intrusive—but still reasonable based upon the circumstances of the investigation – from the available options to obtain the information.

(U) The Privacy Act may not exempt from disclosure information the FBI collects during Positive Foreign Intelligence Assessments and investigations to qualified U.S. citizens or lawfully admitted permanent residents when personally identifying information about such persons resides in those files. FBI employees should therefore be particularly vigilant about properly classifying any such information and avoiding unnecessary references to, and the documentation of, identifying information about U.S. citizens and lawfully admitted permanent residents in Positive Foreign Intelligence files.

9.4 (U) LEGAL AUTHORITY

(U) The FBI's legal authority to collect positive foreign intelligence derives from a mixture of administrative and statutory sources. (See E.O. 12333; 50 U.S.C. §§ 401 et seq.; 50 U.S.C. §§ 1801 et seq.; 28 U.S.C. § 532 note [incorporates the Intelligence Reform and Terrorism Protection Act, P.L. 108-458 §§ 2001-2003]). In collecting positive foreign intelligence, the FBI will be guided by collection requirements issued under the authority of the DNI, including the National Intelligence Priorities Framework and the National Human Intelligence (HUMINT) Collection Directives, or any successor directives issued under the authority of the DNI and accepted by FBIHQ DI (PFI Collection Requirements).

9.4.1 (U) FULL INVESTIGATION ACTIVITIES

(U//FOUO) As discussed in Section 7 of the DIOG, the AGG-Dom cites three predication circumstances warranting a Full Investigation, one of which specifically applies to the collection of positive foreign intelligence: "The Full Investigation may obtain foreign intelligence that is responsive to a [positive] foreign intelligence requirement."

(U//FOUO) A PFI investigation may only be commenced if the Office of the DNI has levied a foreign intelligence collection requirement on the FBI and the DI has accepted the requirement as one to which the FBI will endeavor to respond to as part of its PFI Program (i.e., PFI Collection Requirements). The FBI is authorized to open a Full Investigation to collect on a USIC intelligence requirement only if it has been accepted and designated by FBIHQ DI as a PFI Collection Requirement.

9.5 (U) GENERAL REQUIREMENTS AND FBIHQ STANDARDS FOR APPROVING THE OPENING OF POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS

9.5.1 (U) GENERAL REQUIREMENTS AND PROGRAM RESPONSIBILITIES

(U//FOUO) The DCHMS is responsible for promulgating FBI policy and oversight of the Foreign Intelligence Collection Program (FICP). DCHMS, DCPMU will provide notice to the DOJ NSD upon the opening of a positive foreign intelligence Full Investigation. To ensure that all positive foreign intelligence collection is focused on authorized PFI Collection Requirements, only DCPMU may approve the opening of a Full Investigation (809-814 or 816 classifications). Only personnel assigned to FIGs may conduct PFI Full Investigations. Field offices must request, by EC to the DCPMU Unit Chief (UC) approval to open Full Investigations to collect on PFI Collection Requirements.

(U//FOUO) If at the time of the opening, or at anytime thereafter, the PFI Full Investigation involves a Sensitive Investigative matter (SIM), the title/caption must contain the words "Sensitive Investigative Matter."

(U//FOUO) The DIOG prohibits the use of control files or administrative files to document investigative activity. (See DIOG Appendix J)

9.5.2 (U) STANDARDS FOR OPENING A FULL INVESTIGATION TO COLLECT POSITIVE FOREIGN INTELLIGENCE

(U//FOUO) Before opening or approving a Full Investigation for the purpose of collecting PFI, the approving official must determine whether:

- A) (U//FOUO) The FBI DI has established an PFI Collection Requirement for opening a Full Investigation;
- B) (U//FOUO) The Full Investigation is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only such factors; and
- C) (U//FOUO) The Full Investigation is an appropriate use of personnel and financial resources.

(U//FOUO) Additional policies regarding Predicated Investigation involving any foreign ambassador, foreign official, foreign student or exchange visitor, protected persons or premises as a subject may be found in DIOG Appendix G [No Foreign Policy Objection (NFPO)].

9.6 (U) OPENING DOCUMENTATION, APPROVAL, EFFECTIVE DATE, AND FILE REVIEW

9.6.1 (U) OPENING BY A FIELD OFFICE WITH FBIHQ DCPMU UC APPROVAL OR OPENING BY FBIHQ

(U//FOUO) The predication for a Full PFI Investigation must be documented in the opening electronic communication (EC). A Full PFI Investigation may not be opened on oral authority.

9.6.1.1 (U) APPROVAL TO OPEN A FULL PFI INVESTIGATION

(U//FOUO) Opened by a Field Office or Opened by FBIHQ: DCPMU UC will approve the opening of a Full Investigation based on PFI Collection Requirements.

9.6.1.1.1 (U) EFFECTIVE DATE

(U//FOUO) Opened by a Field Office or Opened by FBIHQ: The effective date of the Full Investigation is the date the DCPMU UC approves the EC by electronic signature/date generated by Sentinel or by handwriting this/her initials and date on the EC.

9.6.1.2 (U) APPROVAL TO OPEN A FULL PFI INVESTIGATION INVOLVING A SENSITIVE INVESTIGATIVE MATTER (SIM)

(U//FOUO) The opening of a Full PFI Investigation involving a SIM:

9.6.1.2.1 (U) SIM FULL PFI INVESTIGATION OPENED BY A FIELD OFFICE

(U//FOUO) The opening in a field office of a Full Investigation to collect PFI involving a SIM must have prior Chief Division Counsel (CDC) review, and approval by the Special Agent in Charge (SAC) and the DCHMS Section Chief (SC). The notice must identify all known SIMs involved in the investigation, and include the caption on the opening

communication – “Sensitive Investigative Matter.” The DCHMS must notify, in writing, the appropriate NSD official as soon as practicable, but no later than 30 calendar days after the opening of the investigation. See the classified provisions in DIOG Appendix G for additional notice requirements.

(U//FOUO) If a SIM arises after the opening of a Full Investigation to collect PFI, the investigation may continue, but the matter must be reviewed by the CDC or OGC and approved by the SAC and DCHMS SC, as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided to DOJ as indicated above.

9.6.1.2.2 (U) SIM FULL PFI INVESTIGATION OPENED BY FBIHQ

(U//FOUO) The opening by FBIHQ of a Full Investigation to collect PFI involving a SIM must have prior OGC review, and approval by the DCHMS SC. The notice must identify all known SIMs involved in the investigation, and include the caption on the opening communication – “Sensitive Investigative Matter.” The DCHMS must notify, in writing, the appropriate NSD official as soon as practicable, but no later than 30 calendar days after the opening of the investigation. See the classified provisions in DIOG Appendix G for additional notice requirements.

(U//FOUO) If a SIM arises after the opening of a Full Investigation to collect PFI, the investigation may continue, but the matter must be reviewed by the OGC and approved by the DCHMS SC, as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Notice must be provided to DOJ as indicated above.

9.6.1.2.3 (U) EFFECTIVE DATE

(U//FOUO) Opened by a Field Office or Opened by FBIHQ: The effective date of the Full Investigation involving a SIM is the date the DCHMS SC approves the EC by electronic signature/date generated by Sentinel or by handwriting their initials and date on the EC.

9.6.2 (U) NOTICE TO DOJ

9.6.2.1 (U) FOR A FULL PFI INVESTIGATION

(U//FOUO) Notice to DOJ is required when a Full Investigation to collect information responsive to a foreign intelligence requirement is opened. Notice must be forwarded from DCHMS, DCPMU to the DOJ NSD as soon as practicable but no later than 30 calendar days after the opening of the investigation. (AGG-Dom, Part II.B.5) For Full PFI Investigations that are a SIM, see DIOG Section 9.6.1.2 above.

9.6.3 (U) DURATION

(U//FOUO) A Full PFI Investigation may continue for as long as necessary until the requirement is met, or the investigation concludes they cannot satisfy the requirement.

9.6.4 (U) FILE REVIEW

9.6.4.1 (U) FULL INVESTIGATIONS

(U//FOUO) Supervisory file reviews of a Full PFI Investigation must be conducted at least every 90 days in accordance with DIOG Section 3.4.4. File reviews for probationary agents must be conducted at least every 60-days.

9.6.5 (U) ANNUAL LETTERHEAD MEMORANDUM

9.6.5.1 (U) FIELD OFFICE RESPONSIBILITY

(U//FOUO) All FIGs must submit an annual report on each Full PFI Investigation that was open for any period of time during the previous calendar year. This report is due to FBIHQ DCHMS no later than January 30th of the calendar year following each year during which a Full Investigation is open and must include the following:

- A) (U//FOUO) The PFI requirement to which the investigation was responding;
- B) (U//FOUO) All methods of collection used;
- C) (U//FOUO) All Sensitive Investigative Matters encountered;
- D) (U//FOUO) A list of all IIRs by number issued based on information collected during the investigation;
- E) (U//FOUO) A summary of the PFI collected; and
- F) (U//FOUO) The date the Full Investigation was opened and, if applicable, the date it was closed.

(U//FOUO) These reports should be submitted by EC. The EC must be uploaded into ACS as designated in the IPG.

9.6.5.2 (U) FBIHQ RESPONSIBILITY

(U//FOUO) DCHMS must compile data from each field office regarding the scope and nature of the prior year's PFI collection program. No later than April 1st of each year, the DCHMS must submit a comprehensive report of all activity described above to DOJ NSD. The report must include the following information:

- A) (U//FOUO) The PFI requirement to which the investigations were responding;
- B) (U//FOUO) All Sensitive Investigative Matters encountered; and
- C) (U//FOUO) The date all Full Investigation were opened and closed (if applicable).

9.7 (U) STANDARDS FOR OPENING OR APPROVING THE USE OF AN AUTHORIZED INVESTIGATIVE METHOD IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//FOUO) Prior to opening or approving the use of an investigative method in a Full Investigation for the purpose of collecting positive foreign intelligence pursuant to a PFI Collection Requirement, an FBI employee or approving official must determine whether:

- A) (U//FOUO) The use of the particular investigative method is likely to further the authorized purpose of the Full Investigation;
- B) (U//FOUO) The investigative method selected is the least intrusive method, if reasonable based upon the circumstances of the investigation and, if taken relative to an US person (USPER), the method involves open and consensual activities, to the extent practicable;
- C) (U//FOUO) Open and consensual activity would likely be successful (if it would, covert non-consensual contact with an USPER may not be approved); and
- D) (U//FOUO) The investigative method is an appropriate use of personnel and financial resources.

9.8 (U) AUTHORIZED INVESTIGATIVE METHODS IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//FOUO) Prior to opening or approving the use of an investigative method, an FBI employee and approving official must apply the standards as provided in DIOG Section 9.7. With the exceptions noted below, all lawful methods may be used during a Full Investigation to collect positive foreign intelligence pursuant to PFI Collection Requirements. If actions are to be taken with respect to an USPER, the method used must be open and consensual, to the extent practicable.

(U) See DIOG Section 18 for a complete description of the following methods that may be used in Full PFI Investigations. The methods are:

- A) (U) Public information. (See Section 18.5.1)
- B) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
- C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
- D) (U) On-line services and resources. (See Section 18.5.4)
- E) (U) CHS use and recruitment. (See Section 18.5.5)
- F) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
- G) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
- H) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- I) (U) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)
- J) (U) Consensual monitoring of communications, including electronic communications. (Section 18.6.1)

(U//FOUO) For those state, local and tribal governments that do not sanction or provide a law enforcement exception available to the FBI for one-party consent recording of communications with persons within their jurisdiction, the SAC must approve the consensual monitoring of communications as an Otherwise Illegal Activity (OIA). Prior to the SAC authorizing the OIA, one-party consent must be acquired. The SAC may delegate the OIA approval authority to an Assistant Special Agent-in-Charge (ASAC) or Supervisory Special Agent (SSA).

(U//FOUO) See the classified provisions in Appendix G for additional information.

- K) (U) Intercepting the communications of a computer trespasser. (Section 18.6.2)
- L) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)
- M)(U) Polygraph examinations. (Section 18.6.11)
- N) (U) Undercover Operations (Section 18.6.13)
- O) (U//FOUO) Pen registers and trap/trace devices for non-USPERs using FISA. (See Section 18.6.9)
- P) (U) Electronic surveillance using FISA or E.O. 12333. (See Section 18.7.3)
- Q) (U//FOUO) Searches – with a warrant or court order using FISA or E.O. 12333 § 2.5. The DIOG classified Appendix G provides additional information regarding certain searches. (AGG-Dom, Part V.A.12) (See Section 18.7.1)
- R) (U) FISA Title VII - Acquisition of positive foreign intelligence information. (See Section 18.7.3)
- S) (U//FOUO) FISA Order for business records (for records relating to a non-USPER only). (See Section 18.6.7)

9.9 (U) INVESTIGATIVE METHODS NOT AUTHORIZED DURING A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//FOUO) The following investigative methods are not permitted to be used for the purpose of collecting positive foreign intelligence pursuant to PFI Collection Requirements:

- A) (U//FOUO) National Security Letters (15 U.S.C. §§ 1681u, 1681v; 18 U.S.C. § 2709; 12 U.S.C. § 341[a][5][A]; 50 U.S.C. § 436). (Section 18.6.6)
- B) (U//FOUO) FISA Order for business records (for records relating to an USPER). (Section 18.6.7)
- C) (U//FOUO) Pen registers and trap/trace devices in conformity with FISA (on an USPER). (Section 18.6.9)
- D) (U//FOUO) Pen registers and trap/trace devices in conformity with chapter 206 of 18 U.S.C. §§ 3121-3127. (Section 18.6.9)
- E) (U//FOUO) Mail covers. (Section 18.6.10)
- F) (U//FOUO) Grand jury subpoenas. (Section 18.6.5)
- G) (U//FOUO) Administrative subpoenas. (Section 18.6.4)

- H) (U//FOUO) Stored wire and electronic communications and transactional records. (Section 18.6.8)

9.10 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM) IN A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

(U//FOUO) The title/caption of the opening or subsequent EC for a Full Investigation for the collection of PFI involving a SIM must contain the words “Sensitive Investigative Matter.” DIOG Section 10 contains the required approval authorities and factors to be considered relative to a Predicated Investigation involving a SIM.

9.10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) A SIM is an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), religious or domestic political organization or individual prominent in such an organization, or news media, an academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials. (AGG-Dom, Part VII.N.) As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary. DIOG Section 10 and/or the classified provisions in DIOG Appendix G define domestic public official, political candidate, religious or political organization or individual prominent in such an organization, and news media.

(U//FOUO) All Full PFI Investigations involving a SIM must be reviewed by the CDC/OGC, approved by the SAC and the DCHMS SC.

9.10.2 (U) ACADEMIC NEXUS

(U//FOUO) As a matter of FBI policy, an investigative activity having an “academic nexus” is considered a SIM if:

- A) (U//FOUO) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under investigation is related to the individual’s position at the institution; or
- B) (U//FOUO) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of “academic freedom” (e.g., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a SIM even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

9.11 (U) RETENTION OF INFORMATION

(U//FOUO) DCHMS must maintain a database or records systems that permits the prompt retrieval of the status of each positive foreign intelligence collection Full Investigation (open or closed), the dates of opening and closing, and the basis for the Full Investigation.

9.12 (U//FOUO) STANDARDS FOR APPROVING THE CLOSING OF A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION

9.12.1 (U) STANDARDS

(U//FOUO) At the conclusion of a Full positive foreign intelligence Investigation, each of the following items must be documented in the closing communication (EC and/or LHM):

- A) (U//FOUO) A summary of the results of the investigation;
- B) (U//FOUO) Whether logical and reasonable investigation was completed (i.e. the matter acquired the positive foreign intelligence information sought);
- C) (U//FOUO) Whether all investigative methods initiated have been completed and/or discontinued;
- D) (U//FOUO) Whether all leads set have been completed and/or discontinued;
- E) (U//FOUO) Whether all evidence has been returned, destroyed or retained in accordance with evidence policy; and
- F) (U//FOUO) A summary statement of the basis on which the foreign intelligence investigation will be closed, and the selection of C-4 for Administrative Closing, which includes:
 - 1) (U//FOUO) No further investigation is warranted and/or leads have been exhausted;
 - 2) (U//FOUO) Investigation assigned a new file number; or
 - 3) (U//FOUO) Investigation consolidated into a new file number or an existing file number.

9.12.2 (U) APPROVAL REQUIREMENTS

(U//FOUO) The appropriate closing supervisor described below must review and approve the closing communication (as described in Section 9.12.1) to ensure it contains the above-required information and sufficient details of the investigation on which to base a decision to close the foreign intelligence investigation. The closing supervisor must note on the closing document "C" (for close), the closing status 4 (e.g., C-4), and the closing date. The appropriate closing supervisors are:

9.12.2.1 (U) OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//FOUO) Closing a Full PFI Investigation opened by a field office requires a written request from the FIG SSA and the approval of the DCPMU UC.

9.12.2.2 (U) OPENED BY FBIHQ

(U//FOUO) Closing a Full PFI Investigation opened by FBIHQ requires approval from the DCPMU UC and notification to the appropriate field office.

9.12.2.3 (U) SIM OPENED BY A FIELD OFFICE WITH FBIHQ APPROVAL

(U//FOUO) Closing a PFI Full Investigation opened by a field office involving a SIM requires approval from the SAC and the DCHMS SC.

9.12.2.4 (U) SIM OPENED BY FBIHQ

(U//FOUO) Closing a PFI Full Investigation opened by FBIHQ involving a SIM requires approval from the DCHMS SC, and written notification to the appropriate field office.

9.13 (U) OTHER PROGRAM SPECIFIC INVESTIGATION REQUIREMENTS

(U//FOUO) To facilitate compliance with investigative program-specific requirements, the FBI employee should consult the relevant division's PG to ascertain any program-specific requirements. However, FBIHQ division PGs may not contradict, alter or otherwise modify the standards established in the DIOG.

10 (U//FOUO) SENSITIVE INVESTIGATIVE MATTER (SIM) AND SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)

10.1 (U) SENSITIVE INVESTIGATIVE MATTERS (SIM)

10.1.1 (U) OVERVIEW

(U) Certain investigative matters should be brought to the attention of FBI management and Department of Justice (DOJ) officials because of the possibility of public notoriety and sensitivity. Accordingly, Assessments and Predicated Investigations involving “sensitive investigative matters” have special approval and reporting requirements.

10.1.2 (U) PURPOSE, SCOPE, AND DEFINITIONS

10.1.2.1 (U) DEFINITION OF SENSITIVE INVESTIGATIVE MATTERS (SIM)

(U//FOUO) A sensitive investigative matter (SIM) is defined as an investigative matter involving the activities of a domestic public official or domestic political candidate (involving corruption or a threat to the national security), a religious or domestic political organization or individual prominent in such an organization, or the news media; an investigative matter having an academic nexus; or any other matter which, in the judgment of the official authorizing the investigation, should be brought to the attention of FBI Headquarters (FBIHQ) and other DOJ officials. (Attorney General’s Guidelines for Domestic FBI Operations (AGG-Dom), Part VII.N.) As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary.

(U//FOUO) The phrase “*investigative matter involving the activities of*” is intended to focus on the behaviors and/or activities of the subject, target, or subject matter of the Assessment or Predicated Investigation. The phrase is generally not intended to include a witness or victim in the Assessment or Predicated Investigation. This definition does not, however, prohibit a determination that the status, involvement, or impact on a particular witness or victim would make the Assessment or Predicated Investigation a SIM under subsection 10.1.2.2.7 below.

10.1.2.2 (U) DEFINITIONS/DESCRIPTIONS OF SIM OFFICIALS AND ENTITIES

(U) Descriptions for each of the officials and entities contained in the SIM definition are as follows:

10.1.2.2.1 (U) DOMESTIC PUBLIC OFFICIAL

(U//FOUO) A domestic public official is an elected official or an appointed official serving in a judicial, legislative, management, or executive-level position in a Federal, state, local, or tribal government entity or political subdivision thereof. A matter involving a domestic public official is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

(U//FOUO) This definition is intended to exclude lower level positions and most line positions, such as a patrol officer or office secretary from the SIM category, but it does include supervisory personnel (e.g., police Sergeant or Lieutenant). The SIM definition also eliminates the “position of trust” language.

10.1.2.2.2 (U) DOMESTIC POLITICAL CANDIDATE

(U//FOUO) A domestic political candidate is an individual who is seeking election to, or nomination for election to, or who has authorized others to explore on his or her behalf the possibility of election to an office in a federal, state, local or tribal governmental entity or political subdivision thereof. As with domestic public officials, a matter involving a political candidate is a SIM if the Assessment or Predicated Investigation involves corruption or a threat to the national security.

10.1.2.2.3 (U) DOMESTIC POLITICAL ORGANIZATION OR INDIVIDUAL PROMINENT IN SUCH AN ORGANIZATION

(U//FOUO) Domestic political organization includes political parties at any level, political action groups or committees, or committees or groups formed for the purpose of electing an individual to public office or to advocate or educate the public concerning a political or social issue. If the Assessment or Predicated Investigation concerns a person prominent in such an organization, but not the organization itself, it must still be treated as a SIM.

10.1.2.2.4 (U) RELIGIOUS ORGANIZATION OR INDIVIDUAL PROMINENT IN SUCH AN ORGANIZATION

(U//FOUO) Religious organization includes any association of persons whose purpose primary is worship (whether in a church, mosque, synagogue, temple, or other meeting location) or other entity whose principal purpose is the study or advancement of religion. Religious organizations may be organized in a variety of ways, such as an unincorporated association, non-profit corporation, charitable trust, or an association in fact. If the Assessment or Predicated Investigation concerns a person prominent in such an organization, but not the organization itself, it must still be treated as a SIM.

10.1.2.2.5 (U) MEMBER OF THE NEWS MEDIA OR A NEWS ORGANIZATION

(U//FOUO) “News media” includes persons and organizations that gather, report, or publish news, whether through traditional means (e.g., newspapers, radio, magazines, news service) or the on-line or wireless equivalent. A “member of the news media” is a person who gathers, reports, or publishes news through the news media.

(U//FOUO) The term “News Media” also includes an entity organized and operated for the purpose of gathering, reporting or publishing news. The definition does not, however, include a person or entity who posts information or opinion on the Internet in blogs, chat rooms or social networking sites, such as YouTube, Facebook, or MySpace, unless that person or entity falls within the definition of a member of the media or a news organization under the other provisions within this section (e.g., a national news reporter who posts on his/her personal blog).

(U//FOUO) Examples of news media entities include television or radio stations broadcasting to the public at large and publishers of newspapers or periodicals that make their products available to the public at large in print form or through an Internet distribution. A freelance journalist may be considered to be a member of the media if the journalist has a contract with the news entity or has a history of publishing content. Publishing a newsletter or operating a website does not by itself qualify an individual as a member of the media. Businesses, law firms, and trade associations offer newsletters or have websites; these are not considered news media. As the term is used in the DIOG, “news media” is not intended to include persons and entities that simply make information available. Instead, it is intended to apply to a person or entity that gathers information of potential interest to a segment of the general public, uses editorial skills to turn raw materials into a distinct work, and distributes that work to an audience, as a journalism professional.

(U//FOUO) If there is doubt about whether a particular person or entity should be considered part of the “news media,” the doubt should be resolved in favor of considering the person or entity to be the “news media.”

(U//FOUO) See the classified provisions in DIOG Appendix G for additional guidance on SIMs.

10.1.2.2.6 (U) ACADEMIC NEXUS

(U//FOUO) As a matter of FBI policy, an investigative activity having an “academic nexus” is a SIM if:

- A) (U//FOUO) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under Assessment/investigation is related to the individual's position at the institution; or
- B) (U//FOUO) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States.

(U//FOUO) The sensitivity related to an academic institution arises from the American tradition of “academic freedom” (i.e., an atmosphere in which students and faculty are free to express unorthodox ideas and views and to challenge conventional thought without fear of repercussion). Academic freedom does not mean, however, that academic institutions are off limits to FBI investigators in pursuit of information or individuals of legitimate investigative interest.

(U//FOUO) For matters not considered a SIM even though there is an academic nexus, see the classified provisions in DIOG Appendix G.

10.1.2.2.7 (U) OTHER MATTERS

(U//FOUO) Any matter that in the judgment of the official authorizing an investigation should be brought to the attention of FBIHQ and other DOJ officials is also a SIM. As a matter of FBI policy, “judgment” means that the decision of the authorizing official is discretionary.

10.1.3 (U) FACTORS TO CONSIDER WHEN OPENING OR APPROVING AN INVESTIGATIVE ACTIVITY INVOLVING A SIM

(U//FOUO) In addition to the standards for approving investigative activity in Sections 5, 6, 7, 8 and 9, the following factors should be considered by (i) the FBI employee who seeks to open an Assessment or Predicated Investigation involving a SIM, as well as by the (ii) Chief Division Counsel (CDC) or Office of the General Counsel (OGC) when reviewing such matters, and (iii) the approving official when determining whether the Assessment or Predicated Investigation involving a SIM should be authorized:

- A) (U//FOUO) Seriousness/severity of the violation/threat;
- B) (U//FOUO) Significance of the information sought to the violation/threat;
- C) (U//FOUO) Probability that the proposed course of action will be successful;
- D) (U//FOUO) Risk of public exposure, and if there is such a risk, the adverse impact or the perception of the adverse impact on civil liberties and public confidence; and
- E) (U//FOUO) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing).

(U//FOUO) In the context of a SIM, particular care should be taken when considering whether the planned course of action is the least intrusive method if reasonable based upon the circumstances of the investigation.

10.1.4 (U) OPENING DOCUMENTATION, APPROVAL, NOTICE, AND CHANGE IN SIM STATUS

(U//FOUO) If at the time of the opening, or at anytime thereafter, the Assessment involves a SIM, the title/caption must contain both the words "Assessment" and "Sensitive Investigative Matter." If at the time of the opening, or at anytime thereafter, the Predicated Investigation involves a SIM, the title/caption must contain the words "Sensitive Investigative Matter." Conversely, if a matter that has been designated as a SIM no longer remains a SIM due to a change in the facts and circumstances of the assessment or investigation, this change of designation must be made in the file and the caption.

(U//FOUO) The following are required approval and notification levels for investigative activities involving SIMs:

10.1.4.1 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS BY A FIELD OFFICE**10.1.4.1.1 (U) TYPE 1 & 2 ASSESSMENTS**

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. A Type 1 & 2 Assessment involving a SIM must be reviewed by the CDC and approved by the Special Agent-in-Charge (SAC) as soon as practicable, but no later than five (5) business days after the opening to authorize the Assessment to continue.

10.1.4.1.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following review and approval to open a Type 3 and 4 Assessment as a SIM: CDC review and SAC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Sections 5.6.3.2.4 and 5.6.3.3.4.)

10.1.4.1.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the SAC's prior approval to open a Type 5 Assessment on a sensitive potential confidential human source (CHS). If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive potential CHS, the Assessment may continue, but the matter must be approved by the SAC as soon as practicable, but no later than five (5) business days after this determination is made to authorize the Assessment to continue. (See DIOG Section 5.6.3.4.4.1)

10.1.4.1.4 (U) TYPE 6 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following review and approval to open a Type 6 Assessment as a SIM: CDC review, SAC approval, and Domain Collection and HUMINT Management Section (DCHMS) Section Chief (SC) approval. If the SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by the CDC and approved by the SAC and DCHMS SC as soon as practicable, but no later than five (5) business days after the SIM arises to authorize the Assessment to continue. (See DIOG Section 5.6.3.5.4)

(U//FOUO) FBIHQ must receive notice and approve all Type 6 Assessments whether or not they involve a SIM.

10.1.4.2 (U) NOTICE FOR SIM ASSESSMENTS BY A FIELD OFFICE

(U//FOUO) Notice for SIM Assessments—There is no requirement to notify FBIHQ, DOJ, or the United States Attorney (USA) of the opening of an Assessment involving a SIM. (AGG-Dom, Part II.B.5.a)

10.1.4.3 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE

10.1.4.3.1 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review and SAC approval. (See Sections 6.10 and 7.10)

10.1.4.3.2 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review, SAC approval, and SC approval. (See Section 8.6)

10.1.4.3.3 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//FOUO) CDC review, SAC approval, and DCHMS SC approval. (See DIOG Sections 9.6 and 9.10)

10.1.4.4 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS BY A FIELD OFFICE**10.1.4.4.1 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS**

(U//FOUO) The field office must provide written notification (EC and a disseminable LHM) to the responsible FBIHQ unit and section within 15 calendar days after the opening of a SIM Predicated Investigation. The field office also must notify the appropriate United States Attorney's Office (USAO), in writing, unless such notification is inappropriate under the circumstances (e.g., a public corruption investigation of a person who is personally close to the United States Attorney (USA), or the matter is a counterintelligence or espionage investigation. (See the CD PG for details concerning notice in counterintelligence and espionage investigations.) If notice is not provided to the USAO under the circumstances described above, the field office must explain those circumstances in the written notice to FBIHQ. The responsible FBIHQ section must notify, in writing, the appropriate DOJ Criminal Division official or NSD official. The notification must be made as soon as practicable but no later than 30 calendar days after the opening of the investigation. The notice must identify all known SIMs involved in the investigation. See the classified provisions in DIOG Appendix G for additional notice requirements.

(U//FOUO) If a SIM arises after the initiation of a Predicated Investigation, investigative activity may continue, but the matter must be reviewed by the CDC and approved by the SAC (and SC, if the matter is an Enterprise Investigation or PFI Full Investigation) as soon as practicable, but not more than five (5) business days thereafter to continue the investigation. Written notice must be furnished to the FBIHQ unit and section and to the appropriate USAO, DOJ Criminal and/or NSD, as specified above.

10.1.4.4.2 (U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS

(U//FOUO) See DIOG Section 8.6 for notice requirements.

10.1.4.4.3 (U) NOTICE FOR SIM POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS

(U//FOUO) See DIOG Section 9.9 for notice requirements.

10.1.4.5 (U) REVIEW AND APPROVAL OF SIM ASSESSMENTS OPENED BY FBIHQ**10.1.4.5.1 (U) TYPE 1 & 2 ASSESSMENTS**

(U//FOUO) An FBI employee may open a Type 1 & 2 Assessment, as described in Section 5.6.3.1, without prior supervisory approval. An Assessment involving a SIM must be reviewed by the OGC and approved by the SC as soon as practicable, but no later than five (5) business days after the opening to continue the Assessment. If a SIM arises after the initiation of an Assessment, investigative activity may continue, but the matter must be reviewed by the

OGC and approved by the SC as soon as practicable, but not more than five (5) business days thereafter to continue the Assessment.

10.1.4.5.2 (U) TYPE 3 AND 4 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following reviews and prior approvals to open a Type 3 or 4 SIM Assessment: OGC review and SC approval. If a SIM arises after the opening of a Type 3 or 4 Assessment, the Assessment may continue, but the matter must be reviewed by the OGC and approved by the SC as soon as practicable, but no later than five (5) business days thereafter to continue the Assessment.

10.1.4.5.3 (U) TYPE 5 ASSESSMENTS

(U//FOUO) An FBI employee must obtain his/her SC's approval to open a Type 5 Assessment on a sensitive potential CHS. If it is determined after the opening of a Type 5 Assessment that the individual is a sensitive potential CHS, the Assessment may continue, but the matter must be approved by the employee's SC as soon as practicable, but no later than five (5) business days after this determination. (See Section 5.6.3.4.4.1)

10.1.4.5.4 (U) TYPE 6 ASSESSMENTS

(U//FOUO) An FBI employee must obtain the following reviews and approvals to open a Type 6 Assessment as a SIM: OGC review and SC approval. If a SIM arises after the opening of a Type 6 Assessment, the Assessment may continue, but the matter must be reviewed by OGC and approved by the SC as soon as practicable, but no later than five (5) business days thereafter to continue the Assessment. (See Section 5.6.3.5.4)

10.1.4.6 (U) NOTICE REQUIREMENTS FOR SIM ASSESSMENTS BY FBIHQ

(U//FOUO) There is no requirement to notify DOJ or the United States Attorney of the opening of an Assessment involving a SIM (including opening a sensitive potential CHS). (AGG-Dom, Part II.B.5.a)

10.1.4.6.1 (U) REVIEW AND APPROVAL OF SIM PREDICATED INVESTIGATIONS BY FBIHQ

10.1.4.6.2 (U) PREDICATED INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Sections 6.7, 6.10; 7.7 and 7.10)

10.1.4.6.3 (U) ENTERPRISE INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Sections 8.6)

10.1.4.6.4 (U) POSITIVE FOREIGN INTELLIGENCE FULL INVESTIGATIONS INVOLVING A SIM

(U//FOUO) OGC review and SC approval. (See DIOG Section 9.9)

10.1.4.7 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS BY FBIHQ**10.1.4.7.1 (U) NOTICE FOR SIM PREDICATED INVESTIGATIONS**

(U//FOUO) The responsible FBIHQ section must provide written notification (EC and a disseminable LHM) to any appropriate field office within 15 calendar days after the opening of a SIM Predicated Investigation; the USAO, unless such notification is inappropriate under the circumstances, or the matter is a counterintelligence or espionage investigation (See the CD PG for details concerning notice in counterintelligence and espionage investigations.); and the appropriate DOJ Criminal Division official or NSD official, as soon as practicable, but no later than 30 calendar days after the opening of the investigation. If notice is not provided to the USAO under the circumstances described above, FBIHQ must explain those circumstances in the written notice to the field office(s) and DOJ. The notice must identify all known SIMs involved in the investigation. See the classified provisions in DIOG Appendix G for additional notice requirements.

(U//FOUO) If a SIM arises after the initiation of a Predicated Investigation, investigative activity may continue, but the matter must be reviewed by OGC and approved by the SC as soon as practicable, but not more than five (5) business days thereafter to further continue the investigation. Written notice must be furnished to the appropriate USAO, DOJ Criminal Division and/or NSD, as specified above.

10.1.4.7.2 (U) NOTICE FOR SIM ENTERPRISE INVESTIGATIONS

(U//FOUO) See DIOG Section 8.6 for notice requirements.

10.1.4.7.3 (U) NOTICE FOR SIM FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATIONS

(U//FOUO) See DIOG Section 9.9 for notice requirements.

10.1.4.8 (U) CHANGE IN SIM STATUS

(U//FOUO) If during an Assessment or Predicated Investigation it is determined that the matter is no longer a SIM, an EC or similar document removing the SIM designation from the investigation must be filed setting forth the change in circumstances justifying removal of the SIM designation. The designation of "Sensitive Investigative Matter" will no longer be necessary in future communications (e.g., will no longer appear in the caption or the synopsis section of an EC).

10.1.4.8.1 (U) DOCUMENTATION

(U//FOUO) The FBI employee must:

- A) (U//FOUO) **In Type 1 & 2 Assessments:** Submit an updated FD-71 or Guardian that removes the "Sensitive Investigative Matter" option on the form. The FD-71 or Guardian must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required.

- B) (U//FOUO) **In Type 3 through 6 Assessments:**

- 1) (U//FOUO) Opened by a Field Office - Submit an EC (for Type 5 Assessments, an EC or a successor form in DELTA) that must be approved by the supervisor responsible for the Assessment, reviewed by the CDC, and approved by the SAC. No notice to FBIHQ is required.
 - 2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.
- C) (U//FOUO) **Predicated Investigations:**
- 1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC. For Predicated Investigations, notification must be provided to the same FBIHQ entities (appropriate Unit and Section) that received notice of the SIM.
 - 2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.
- D) (U//FOUO) **Enterprise Investigations:**
- 1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the supervisor responsible for the investigation, reviewed by the CDC, and approved by the SAC and the appropriate SC.
 - 2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the SC.
- E) (U//FOUO) **Positive Foreign Intelligence Full Investigations:**
- 1) (U//FOUO) Opened by a Field Office - Submit an EC that must be approved by the appropriate supervisor, reviewed by the CDC, approved by the SAC and the appropriate DI UC.
 - 2) (U//FOUO) Opened by FBIHQ - Submit an EC that must be approved by the appropriate UC responsible for the investigation, reviewed by OGC, and approved by the DI SC.

10.1.4.9 (U) CLOSING SIM INVESTIGATIONS

10.1.4.9.1 (U) SIM ASSESSMENTS CLOSED BY A FIELD OFFICE

- A) (U//FOUO) **Type 1 & 2 Assessments** - These SIM Assessments must be closed on the FD-71 or FD-71a (Guardian) with approval of the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.1)
- B) (U//FOUO) **Type 3, 4, and 5 Assessments** - The closing EC (or successor form in DELTA for Type 5 Assessments) must be approved by the supervisor responsible for the investigation and the SAC. (See DIOG Section 5.6.3.2, 3, and 4)
- C) (U//FOUO) **Type 6 Assessments** - The closing EC must be approved by the supervisor responsible for the investigation, SAC and the DI SC. (See DIOG Section 5.6.3.5)

10.1.4.9.2 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY A FIELD OFFICE

(U//FOUO) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and foreign intelligence Full Investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

10.1.4.9.3 (U) SIM ASSESSMENTS CLOSED BY FBIHQ

- A) (U//FOUO) Type 1 & 2 Assessments - May be closed on the FD-71 or FD-71a (Guardian) with the approval of the UC responsible for the investigation and his/her SC.
- B) (U//FOUO) Type 3, 4, and 5 Assessments - The closing EC (or successor form in DELTA for Type 5 Assessments) must be approved by the UC responsible for the investigation and his/her SC.
- C) (U//FOUO) Type 6 Assessments - The closing EC must be approved by the DI UC responsible for the investigation and his/her DI SC.

10.1.4.9.4 (U) SIM PREDICATED INVESTIGATIONS CLOSED BY FBIHQ

(U//FOUO) The closing standards, approvals and notice requirements for SIM Predicated Investigations, including Enterprise Investigations and Full foreign intelligence investigations, are specified in DIOG Sections 6.12; 7.12; 8.9; and 9.12 above.

10.1.5 (U) DISTINCTION BETWEEN SIM AND SENSITIVE CIRCUMSTANCE IN UNDERCOVER OPERATIONS

(U//FOUO) The term “sensitive investigative matter,” as used in the DIOG, should not be confused with the term “sensitive circumstance,” as that term is used in undercover operations. “Sensitive circumstance” relates to an undercover operation requiring FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the Attorney General’s Guidelines on FBI Undercover Operations and in Section 18 of the DIOG. The Criminal Undercover Operations Review Committee (CUORC) and the national security Undercover Review Committee (UCRC) must review and approve undercover operations that involve sensitive circumstances. The policy for undercover operations is described in DIOG Section 18.6.13, the Field Guide for Undercover and Sensitive Operations (FGUSO), National Security Undercover Operations Policy Implementation Guide (NSUCOPG), and the FBIHQ operational division program implementation guides.

10.1.6 (U) DISTINCTION BETWEEN SIM AND SENSITIVE UNDISCLOSED PARTICIPATION

(U//FOUO) The term “sensitive investigative matter,” as used in the DIOG, should not be confused with “sensitive UDP (undisclosed participation).” The rules regarding “sensitive investigative matter” and “sensitive UDP” (see DIOG Section 16.2.3.5), while similar, must be applied independently. The SIM designation applies to the overall investigation of which FBI and DOJ officials should be aware due to potential public notoriety and sensitivity. Sensitive UDP, on the other hand, applies to participation by employees or CHSs in lawful organizations that are designated as sensitive. Sensitive UDP can occur in either SIM or non-SIM designated investigations because sensitive UDP focuses on the activity (UDP) - not on the type of investigation in which it is taking place. Certain investigative or intelligence activity, particularly in situations involving academic institutions or student groups, may be covered by one or both these rules. The following scenarios demonstrate how these policies are to be applied:

10.1.6.1 (U) SCENARIOS

(U//FOUO) Scenario 1: An undercover employee (UCE) or confidential human source (CHS) registers as a student at a university and attends classes as part of an investigation of a professor who is alleged to be participating in fraud regarding a federal grant for his academic research.

(U//FOUO) Response 1: This activity would constitute a SIM because it is an investigative matter involving the activities of a faculty member employed by a university located in the United States and the matter under investigation is related to his position. This would also involve sensitive UDP because the UCE or CHS would be participating in the activities of the academic institution in an undisclosed capacity while registering and attending classes. See Section 16.2.3.A.

(U//FOUO) Scenario 2: A UCE or CHS registers and attends classes at a university in order to assist in the investigation of the activities of a professor, who is the subject of an international terrorism investigation unrelated to his status as a professor.

(U//FOUO) Response 2: This investigation would not constitute a SIM, because the investigation does not involve the activities of a university administrator or faculty member related to his position at the institution, nor does the matter involve any student association recognized and approved by the institution. This matter would, however, involve a sensitive UDP, because the UCE or CHS would be participating in the activities of the academic institution in an undisclosed capacity while registering and attending classes.

(U//FOUO) Scenario 3: A domestic public official is alleged to have taken kickbacks from a local contractor for a large construction project. An employee attends a public meeting of the zoning board (chaired by the public official) to see if the contractor will try to meet with the public official.

(U//FOUO) Response 3: This investigation would constitute a SIM because it is focusing on the allegations of corruption by a public official. The employee's attendance at the public board meeting is not sensitive UDP, because the employee is at public event on the same terms and conditions as members of the general public.

10.2 (U//FOUO) SENSITIVE OPERATIONS REVIEW COMMITTEE

(U//FOUO) At the request of the Director, a new joint DOJ/ FBI oversight committee, the Sensitive Operations Review Committee (SORC), has been established to review and monitor certain aspects of FBI investigative activities that are not within the purview of other oversight committees, particularly with regard to Assessments. The SORC is described as follows:

10.2.1 (U) MEMBERSHIP AND STAFFING

A) **(U//FOUO) Chair:** An Executive Assistant Director from the National Security Branch (NSB) or Criminal Cyber Response Services Branch (CCRSB)-depending on which program has the majority of activities being reviewed at the session.

B) **(U) Members:**

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- 1) (U//FOUO) **FBI:** Assistant Directors or designated Deputy Assistant Directors for the Counterterrorism Division, Counterintelligence Division, Cyber Division, Criminal Investigative Division and Directorate of Intelligence; General Counsel; Assistant Director of the Office of Integrity and Compliance; Assistant Director of the Inspection Division; and any other appropriate representative, given the issue presented to the SORC.
- 2) (U//FOUO) **DOJ:** Assistant Attorneys General of the National Security Division (NSD) and the Criminal Division (CRM) or their senior-level designees, and any other appropriate representative, given the issue being considered by the SORC.
- C) (U//FOUO) **Advisors:** The Unit Chief or a designee of the FBI's Corporate Policy Office (CPO) will serve as a policy advisor to the SORC. In addition, DOJ's Chief Privacy and Civil Liberties Officer or a designee will also serve as an advisor to the SORC.
- D) (U//FOUO) **Staff:** The staff of the SORC shall be from the executive staffs of the Executive Assistant Directors of the NSB and the CCSB. Proposals from the NSB shall be handled by its executive staff; proposals from CCSB shall be handled by its executive staff. The staffs will be collectively referred to here as "SORC Staff." The SORC Staff is responsible for ensuring that FBI and DOJ members of the SORC have the information required to perform their SORC duties and are kept fully informed of process developments in matters reviewed by the SORC.

10.2.2 (U) FUNCTION

(U//FOUO) The SORC will review and provide recommendations to the Director on matters submitted, as described below.

10.2.3 (U) REVIEW AND RECOMMENDATION

(U//FOUO) The SORC shall review sensitive activities in the categories described below and provide recommendations to the Director, who shall be the approval authority:

- A) (U//FOUO) Except for Sensitive Undisclosed Participation (sensitive UDP) conducted as part of an authorized Group I Undercover Operation, all requests for authorization for a confidential human source (CHS) to engage in sensitive UDP or for an FBI employee to engage in sensitive UDP that is intended to influence the exercise of First Amendment rights by members of the organization or when the sensitive UDP has been judged by the Office of the General Counsel (OGC) as likely to influence the exercise of First Amendment rights by members of the organization, regardless of prior membership or participation status by the CHS or FBI employee;
(U//FOUO) *Note:* Criminal Undercover Operations Review Committee (CUORC) and National Security Branch (NSB) Undercover Review Committee (UCRC) must provide notice to the SORC of all approved Group I Undercover Operations that include sensitive UDP.
- B) (U//FOUO) Any activity in the United States that is likely to have a significant impact on matters within the jurisdiction of another country, which is conducted without notice to that country and which is not reviewed under another formal process;
- C) (U//FOUO) Any FBI Headquarters (FBIHQ)-directed national or regional Assessment or intelligence collection initiative that could be perceived as ethnic or racial profiling by a reasonable member of the American public with knowledge of the facts and circumstances available or likely to be available to the public;

- D) (U//FOUO) Any proposed Assessment, Predicated Investigation, or intelligence collection, not subject to review under other formal processes that, in the judgment of the official authorizing the activity, could be perceived by a reasonable member of the American public with knowledge of the facts and circumstances available or likely to be available to the public as an unwarranted intrusion into the privacy or civil liberties of United States persons (USPERs), or that poses a significant risk of civil liability against the United States or individual federal employees; or
- E) (U//FOUO) Other matters of a highly sensitive nature that will not be reviewed through other review mechanisms and which, in the judgment of the official authorizing the activity, should be reviewed by the SORC. For example, in criminal matters, *The Attorney General Guidelines on FBI Undercover Activities* (AGG-UCO), Paragraph IV.D.6 provides a review opportunity and process for sensitive investigative matters. A DOJ or FBI official authorized to refer matters under that paragraph should consider whether the matter is limited to the use of an undercover employee, CHS or cooperating subject. If so, the matter should be referred to the CUORC. Other matters having a broader impact on FBI investigative policy or activities should be referred to the SORC.

10.2.3.1 (U) FACTORS TO CONSIDER FOR REVIEW AND RECOMMENDATION

(U//FOUO) In addition to factors unique to the proposal being considered, the SORC will consider the following in determining whether to recommend that a proposed activity be approved:

- A) (U//FOUO) Seriousness/severity of the violation/threat being investigated;
- B) (U//FOUO) Significance of the information sought to the violation/threat being investigated;
- C) (U//FOUO) Probability that the proposed course of action will be successful;
- D) (U//FOUO) Risk of public exposure, and if there is such a risk, the likely impact on public confidence in the FBI;
- E) (U//FOUO) Whether, and the extent to which, the proposed course of action may impact civil liberties, privacy, or constitutional rights;
- F) (U//FOUO) Risk to the national security or the public welfare if the proposed course of action is not approved (i.e., risk of doing nothing);
- G) (U//FOUO) Whether relevant legal and policy restrictions have been identified and considered and the investigators have a plan to address such issues;
- H) (U//FOUO) Whether there are less intrusive feasible means reasonably available; and
- I) (U//FOUO) Whether reasonable mitigation measures have been considered and imposed.

10.2.3.2 (U) PROCESS FOR REVIEW AND RECOMMENDATION

(U//FOUO) The immediate nature of investigating sensitive matters necessitates quick action on proposals. Accordingly, the entire SORC process should, absent unusual circumstances, be completed within 30 calendar days of the initial submission by the field office or FBIHQ.

(U//FOUO) A field office or FBIHQ component must submit a proposal by electronic communication (EC) to the applicable FBIHQ operational division section chief. The FBIHQ operational division must forward the proposal to OGC within 3 business days. The field

office is encouraged to consult with the operational division regarding the merits of the proposal before submitting it in order to facilitate expeditious processing at FBIHQ.

- A) (U//FOUO) The applicable FBIHQ operational division must consult with the OGC to determine whether there are any legal or significant policy prohibitions to the proposed activity, to include whether the activity is likely to influence the exercise of First Amendment rights by members of an organization. Within 5 business days the OGC must determine whether there are any legal prohibitions to the proposed activity. If there are none, OGC must submit the proposal to the SORC Staff. If OGC raises policy concerns, OGC must include an addendum to the proposal describing those concerns to the SORC staff.
- B) (U//FOUO) Upon receipt of the EC and OGC's authorization to submit the proposal, the SORC Staff must place the proposal on the agenda for the next SORC meeting. SORC meetings are scheduled monthly but can be supplemented by ad hoc meetings if necessary.
- C) (U//FOUO) Seven calendar days prior to a scheduled SORC meeting, the SORC Staff must circulate the agenda and pending proposals to SORC members. Each proposal must contain all relevant information, including the following: a detailed description of the proposal; the proponent's explanation for the proposal and an estimate of the period of time for which it would be maintained; OGC's analysis of any significant policy concerns to the proposed activity; and a description of procedures to minimize the acquisition, retention, and dissemination of information regarding USPERs that does not relate to the matter under investigation or to other authorized FBI purposes but that might be incidentally collected and retained absent such procedures. In the case of an ad hoc meeting, the proposal requiring review should be circulated at least 24 hours prior to the meeting.
- D) (U//FOUO) SORC meetings are to be conducted with the expectation that recommendations will be issued when proposals are presented. If discussion reveals that additional information is required to formulate a recommendation, the SORC Staff is required to facilitate access to all information requested by the SORC or by any SORC member. Because SORC members will receive proposal materials in advance and have the opportunity to consult with appropriate FBI or DOJ personnel prior to meeting on a proposal, SORC members, or assistants attending meetings in their place, are expected to make a recommendation on the proposals at the meeting. [Note: Meetings that do not result in a recommendation on a proposal because members wish to consult others prior to acting should be rare.]
- E) (U//FOUO) If there is no consensus among the SORC members on whether the proposal should be approved, the SORC recommendation must provide a fair recitation of the divergent views.
- F) (U//FOUO) Once the SORC has made its recommendation, the SORC Staff must submit the proposal through the appropriate Executive Assistant Director to the Director with the SORC's recommendation for approval or disapproval, together with any changes or amendments to the proposal that the SORC recommends.
- G) (U//FOUO) For each proposal, at the next SORC meeting the SORC Staff must ensure that SORC members are notified whether the Director decided to adopt the recommendation, reject the recommendation, or consult with the Office of the DAG. Should the Director adopt a proposal that either the Assistant Attorney General of the NSD or the Assistant Attorney General of the CRM (or one of their designees) has recommended against, the SORC Staff must notify the relevant Assistant Attorney(s) General. By EC, SORC Staff must notify the submitting office and sponsoring division in a timely manner of the Director's decision.

10.2.4 (U) EMERGENCY AUTHORIZATION

(U//FOUO) When necessary to seize an operational opportunity, in investigations where SORC consideration and Director approval would otherwise be required, emergency approval may be granted by the SAC or FBIHQ Deputy Assistant Director with written notice to the SORC Staff within 48 hours of granting such approval. Unless a SORC member objects to the operation upon receiving such notice from the SORC Staff, the operation may continue until it is reviewed at the next scheduled SORC meeting, when the SORC must make a formal recommendation to the Director whether the activity should continue. If, however, a SORC member objects to the operation upon receiving notice, an ad hoc meeting must be called.

10.2.4.1 (U) NOTICE/OVERSIGHT FUNCTION OF SORC

(U//FOUO) To facilitate its ability to review and provide recommendations to the Director about certain sensitive UDP as described in paragraph C.1, above, the SORC will also receive notice by EC of the following other forms of UDP:

- A) (U//FOUO) In a Predicated Investigation involving non-sensitive UDP, any approval to task a CHS or FBI employee to engage in UDP that (1) is intended to influence the exercise of First Amendment rights by members of the organization; or (2) OGC has determined is likely to influence the exercise of First Amendment rights by members of the organization.
- B) (U//FOUO) In a Predicated Investigation involving either sensitive or non-sensitive UDP, any approval to task a CHS or FBI employee to engage in UDP that may influence the exercise of First Amendment rights by members of the organization but which OGC has determined is not likely to influence the exercise of such rights.
- C) (U//FOUO) In a Predicated Investigation involving sensitive UDP, any approval to task a CHS or FBI employee to engage in UDP that will influence the activities of an organization but which OGC has determined is not likely to influence the exercise of First Amendment rights by members of the organization.
- D) (U//FOUO) In an Assessment or Predicated Investigation involving sensitive UDP, any approval to task a CHS or FBI employee to join an organization or participate in its activities and obtain information.
- E) (U//FOUO) In an Assessment involving sensitive UDP, any approval to task a CHS to obtain information that is not generally known to regular members or participants, regardless of prior membership or participation.

(U//FOUO) *Note:* Notices of UDP falling into any of the above-listed categories must be provided by the approving official by EC to the appropriate SORC staff within 10 days of approval. The SORC members and chairs will receive periodic reports on such UDP from the SORC staff on a schedule and in a form to be determined by the SORC.
- F) (U//FOUO) The SORC may task FBI divisions or field offices to provide it:
 - 1) (U//FOUO) Information regarding any FBI investigative activity that will assist in its oversight function;
 - 2) (U//FOUO) Information regarding any Assessment involving a sensitive investigative matter (SIM) that has received unwanted or unfavorable press exposure; and
 - 3) (U//FOUO) Information regarding operations designated as national security special events.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§10

G) (U//FOUO) The SORC must receive notice of any proposal to use pattern-based data mining queries or other analysis of electronic databases using two or more search criteria designed to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals (as defined in Corporate Policy Directive 0310D). This includes data mining conducted during counterintelligence Assessments or investigations or other national security matters. Any such analysis based solely on racial, ethnic, national origin or religious characteristics is strictly prohibited. A Privacy Threshold Analysis (PTA) for the activity must be completed and forwarded to the Privacy and Civil Liberties Unit, OGC, in conjunction with notifying SORC of the pattern-based data mining. (Note: For purposes of this requirement, pattern-based data mining does not include activities using one or more personal identifiers to identify an individual or analysis designed to discover links between a specific subject and unknown individuals or entities, even if the subject's actual identity is not yet known. Pattern-based data mining does not include queries or analysis designed solely to identify human sources of intelligence nor does it include activities designed to identify an individual or individuals associated with criminal or terrorist activity that has already occurred. For example, database queries using multiple criteria to identify foreign visitors to the United States of a certain age and gender from specific foreign countries who may engage in espionage is pattern-based data mining within the meaning of the statute. In contrast, database queries using criteria such as physical description and motor vehicle ownership to identify possible suspects in a kidnapping do not constitute pattern-based data mining, because the queries are being used to investigate a crime that has already occurred. Queries designed to identify individuals or entities who have had contact with a specific individual are not pattern-based data mining; rather, such queries are subject-based data mining, even if the specific individual's actual identity is presently unknown.

H) (U//FOUO) Senior Executives from the FBI or DOJ may submit other items to the SORC as deemed appropriate to the executive.

10.2.5 (U) LOGISTICS

(U//FOUO) The Executive Assistant Director for the NSB is responsible for all logistical support required for the proper functioning of the SORC (i.e., schedule meetings, provide place for meetings, draft agendas, record keeping and retention functions, all necessary communications, etc.). The CPO and the OGC will assist in establishing the logistical support required for the SORC.

11 (U) LIAISON ACTIVITIES AND TRIPWIRES

11.1 (U) OVERVIEW

(U//FOUO) FBI employees are encouraged to engage in liaison with the general public, private entities, and with local, state, federal, tribal, and foreign government agencies for the purpose of building partnerships. As part of our liaison, community outreach, or investigative/intelligence mission, FBI employees may also establish tripwires with public entities, private entities, and other governmental agencies. Liaison and tripwire initiatives are mutually beneficial for the FBI and the public not only because they help build cooperative relationships and educate about suspicious activities or potential threats, but also because they encourage the public to contact the FBI should they become aware of such suspicious activities or threats.

11.2 (U) PURPOSE AND SCOPE

(U//FOUO) The FBI is authorized to engage in liaison activities and tripwire. The procedures for liaison and setting tripwires, together with documentation and requirements for an Assessment or Predicated Investigation are set forth below.

11.3 (U) APPROVAL REQUIREMENTS FOR LIAISON AND TRIPWIRES

(U//FOUO) Conducting liaison activities or tripwire initiatives do not require approval or the opening of an Assessment or Predicated Investigation unless they use an investigative method set forth in DIOG Sections 18.5 – 18.7. Liaison and Tripwire initiatives may be conducted as part of an already-opened Assessment or Predicated Investigation.

11.3.1 (U) SCENARIO 1

(U//FOUO) An FBI employee makes contact with a chemical supply company to introduce himself/herself and educate the owner about the Bureau's investigative focus on the illegal use of precursor chemicals to make improvised explosive devices. The employee advises the owner to contact the FBI if he/she observes any unusual or suspicious purchases of certain precursor chemicals.

(U//FOUO) **Response:** Such a contact would not require approval or the opening of an Assessment or Predicated Investigation because no investigative methods are used to conduct this activity.

11.3.2 (U) SCENARIO 2

(U//FOUO) Using the same facts as above, except the FBI employee interviews the owner about recent purchases of precursor chemicals and requests the owner to voluntarily produce copies of all purchase records.

(U//FOUO) **Response:** This differs from scenario #1 above because it uses investigative methods described in the AGG-Dom and DIOG Section 18 (interview and request information from

members of the public). To conduct such activity (whether called liaison or setting a tripwire) would require an Assessment or a Predicated Investigation to be open.

11.4 (U) DOCUMENTATION & RECORDS RETENTION REQUIREMENTS

(U//FOUO) The terms “liaison” and “tripwire” have been defined in various ways and may differ by FBIHQ division, program, or field office. Not every contact with a member of the public will be considered liaison activity or a tripwire initiative that needs to be documented. As stated above, employees are encouraged to engage and converse with the public as part of their routine FBI investigative and intelligence mission.

(U//FOUO) Often, however, these terms are used and/or defined in a formal policy or EC to accomplish a particular investigative or intelligence objective. When an employee is directed by a supervisor, FBI policy, or a FBIHQ division to establish a liaison relationship or set a tripwire, that directive, as well as the actions taken by the employee, must be documented with an FD-999. If an employee on his or her own initiative contacts a member of the public and subsequently determines the contact was a liaison or tripwire activity, the contact must be documented using the FD-999. Any questions regarding whether the employee’s contact with the public should be documented as liaison or tripwire activities should be directed to the employee’s supervisor. The intent of this section is to ensure that contacts with the public which are considered to be liaison activities or a tripwire initiatives be documented with the FD-999 into a single database system for tracking and reporting purposes.

(U//FOUO) When the FD-999 is used to document liaison activities or tripwire initiatives, it must be uploaded to file number 319X-HQ-A1487718. Copies of the FD-999 must also be filed as follows:

- A) (U//FOUO) **No Investigative Methods Used:** If no investigative methods (DIOG Sections 18.5 - 18.7) are used in the liaison activity or tripwire, the FD-999 may be uploaded into an investigative file or control file.
- B) (U//FOUO) **Investigative Methods Used:** If investigative methods (DIOG Sections 18.5- 18.7) are used in the liaison activity or tripwire, the FD-999 must also be uploaded in one of the following:
 - 1) (U//FOUO) an Assessment file;
 - 2) (U//FOUO) a Predicated Investigation file;
 - 3) (U//FOUO) a domestic police cooperation file (343 classification);
 - 4) (U//FOUO) a foreign police cooperation file (163 classification); or
 - 5) (U//FOUO) a technical assistance control file (if only technical assistance is provided).

12 (U) ASSISTANCE TO OTHER AGENCIES

12.1 (U) OVERVIEW

(U//FOUO) Part II of the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) authorizes the FBI to conduct investigations in order to detect or obtain information about, and prevent and protect against, federal crimes and threats to the national security and to collect foreign intelligence. (See DIOG Section 2.) Section 12 does not apply to assistance the FBI may provide to other agencies while conducting joint investigations. In such instances, other sections of the DIOG dealing with Assessments and Predicated Investigations would apply.

(U//FOUO) Section 12 specifically addresses those situations in which the FBI has been requested or is seeking to provide assistance to other agencies and does not have an open Assessment or Predicated Investigation. Part III of the AGG-Dom, Assistance to Other Agencies, authorizes the FBI to provide investigative assistance to other federal, state, local or tribal, or foreign agencies when the investigation has the same objectives as Part II of the AGG-Dom or when the investigative assistance is otherwise legally authorized. Accordingly, FBI employees may provide assistance even if it is not for one of the purposes identified as grounds for an FBI investigation or Assessment if providing the assistance is otherwise authorized by law. For example, investigative assistance is legally authorized in certain contexts to state or local agencies in the investigation of crimes under state or local law, as provided in 28 U.S.C. § 540—felonious killing of state and local law enforcement officer; 28 U.S.C. § 540A—violent crime against travelers; 28 U.S.C. § 540B—serial killings, and to foreign agencies in the investigation of foreign law violations pursuant to international agreements. The FBI may use appropriate lawful methods in any authorized investigative assistance activity.

12.2 (U) PURPOSE AND SCOPE

(U) The FBI may provide investigative and technical assistance to other agencies as set forth below.

12.2.1 (U) INVESTIGATIVE ASSISTANCE

(U) The AGG-Dom permits FBI personnel to provide investigative assistance to:

- A) (U) Authorized intelligence activities of other United States Intelligence Community (USIC) agencies;
- B) (U) Any federal agency in the investigation of federal crimes, threats to the national security, foreign intelligence collection, or any other purpose that may be lawfully authorized;
- C) (U) Assist the President in determining whether to use the armed forces pursuant to 10 U.S.C. §§ 331-33, when authorized by Department of Justice (DOJ), as described in Section 12.3.2.2.1.1, below;
- D) (U) Collect information necessary to facilitate public demonstrations and to protect the exercise of First Amendment rights and ensure public health and safety, when authorized by DOJ and done in accordance with the restrictions described in Section 12.3.2.2.1.2, below;

- E) (U) State or local agencies in the investigation of crimes under state or local law when authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);
- F) (U) State, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized;
- G) (U) Foreign agencies in the investigations of foreign law violations pursuant to international agreements, and as otherwise set forth below, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US Person (USPER); and
- H) (U) The Attorney General has also authorized the FBI to provide law enforcement assistance to state or local law enforcement agencies when such assistance is requested by the governor of the state pursuant to 42 U.S.C. § 10501 (for example, federal law enforcement assistance following Hurricane Katrina). The Attorney General must approve any request for assistance under 42 U.S.C. § 10501.

(U) The procedures for providing investigative assistance, together with the standards, approval, notification, documentation, and dissemination requirements are set forth in Sections 12.3, 12.5, and 12.6 below.

12.2.2 (U) TECHNICAL ASSISTANCE

(U) The FBI is authorized to provide technical assistance to all duly constituted law enforcement agencies, other organizational units of the DOJ, and other federal agencies and to foreign governments (to the extent not prohibited by law or regulation). The procedures for providing technical, together with the approval, notification, documentation, and dissemination requirements are set forth in Sections 12.4, 12.5 and 12.6 below.

12.3 (U) INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES - STANDARDS, APPROVALS AND NOTICE REQUIREMENTS

(U) The FBI may provide investigative assistance to other agencies by participating in joint operations and investigative activities with such agencies. (AGG-Dom, Part III.E.1)

(U//FOUO) Dissemination of information to other agencies must be consistent with Director of National Intelligence (DNI) directives, the AGG-Dom, DIOG Section 14, FBI Foreign Dissemination Manual, the Privacy Act of 1974, and any applicable memoranda of understanding/agreement (MOU/MOA), laws, treaties or other policies. (See Sections 12.5 and 12.6 below for documentation and dissemination of information requirements.)

12.3.1 (U) STANDARDS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES

(U//FOUO) The determination whether to provide FBI assistance to other agencies is discretionary but may only occur if:

- A) (U//FOUO) The assistance is within the scope authorized by the AGG-Dom, federal laws, regulations, or other legal authorities;

- B) (U//FOUO) The investigation being assisted is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only these factors; and
- C) (U//FOUO) The assistance is an appropriate use of FBI personnel and financial resources.

12.3.2 (U) AUTHORITY, APPROVAL AND NOTICE REQUIREMENTS FOR PROVIDING INVESTIGATIVE ASSISTANCE TO OTHER AGENCIES

(U//FOUO) Investigative assistance that may be furnished to other agencies is described below by agency type.

12.3.2.1 (U) INVESTIGATIVE ASSISTANCE TO UNITED STATES INTELLIGENCE COMMUNITY (USIC) AGENCIES

12.3.2.1.1 (U) AUTHORITY

- A) (U//FOUO) The FBI may provide investigative assistance (including operational support) for authorized intelligence activities of other USIC agencies. (AGG-Dom, Part III.A)
- B) (U//FOUO) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable. For example, specific approval and notification requirements exist for assisting the Central Intelligence Agency (CIA) and the Department of Defense (DOD) domestic activities.

12.3.2.1.2 (U) APPROVAL REQUIREMENTS

- A) (U//FOUO) **General:** If assistance to a component of the USIC will involve the use of investigative methods other than those authorized for Assessments (those in DIOG Sections 18.6 - 18.7), prior SSA approval must be obtained with the FD-999. Supervisory approval for use of investigative methods authorized only for use during Predicated Investigations shall be at the same level required for the use of that investigative method during an FBI investigation as provided in DIOG Sections 18.6 - 18.7. Approval for use of specific technologies is set forth in Section 12.4 below.
- B) (U//FOUO) **Sensitive Investigative Matters (SIM):** Any investigative assistance to other USIC agencies involving a SIM requires Chief Division Counsel (CDC)/Office of the General Counsel (OGC) review, SAC/Section Chief (SC) approval, and notification, as specified in 12.3.2.1.3.B, below.

12.3.2.1.3 (U) NOTICE REQUIREMENTS

- A) (U//FOUO) **General:** Notice must be provided for the investigative activity or investigative method as specified in the DIOG or applicable MOU/MOAs.
- B) (U//FOUO) **Sensitive Investigative Matters (SIM):** In addition to the above-required approvals, any investigative assistance to USIC agencies involving a SIM requires notification to the appropriate FBI Headquarters (FBIHQ) operational Unit Chief (UC) and SC by Electronic Communication (EC) as soon as practicable, but no later than 15 calendar days after the initiation of the investigative assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or National Security Division (NSD) as soon as practicable, but no later than 30 calendar days after the initiation of any investigative assistance involving a SIM.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- C) (U//FOUO) Classified Appendix: See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.1.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) to USIC agencies using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.2 (U) INVESTIGATIVE ASSISTANCE TO OTHER UNITED STATES FEDERAL AGENCIES

12.3.2.2.1 (U) AUTHORITY

- A) (U//FOUO) The FBI may provide investigative assistance to any other federal agency in the investigation of federal crimes or threats to the national security or in the collection of positive foreign intelligence. (Pursuant to DIOG Section 9, collection of positive foreign intelligence requires prior approval from the Collection Management Section (CMS), FBIHQ.) The FBI may provide investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the United States Secret Service (USSS) in support of its protective responsibilities. (AGG-Dom, Part III.B.1) See DIOG Section 12.4 below for guidance in providing technical assistance to federal agencies.
- B) (U//FOUO) Investigative assistance must be in compliance with interagency MOU/MOA, if applicable.

12.3.2.2.1.1 (U) ACTUAL OR THREATENED DOMESTIC CIVIL DISORDERS

- A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. §§ 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as (AGG-Dom, Part III.B.2):
- 1) (U) The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area;
 - 2) (U) The potential for violence;
 - 3) (U) The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder;
 - 4) (U) The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders; and
 - 5) (U) The extent of state or local resources available to handle the disorder.
- B) (U) Civil disorder investigations will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.
- C) (U) The only investigative methods that may be used during a civil disorder investigation are:
- 1) (U) Public information (See DIOG Section 18.5.1);

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§12

- 2) (U) Records or information - FBI or DOJ (See DIOG Section 18.5.2);
- 3) (U) Records or information - Other Federal, state, local, or tribal, or foreign governmental agency (See DIOG Section 18.5.3);
- 4) (U) Online services and resources (See DIOG Section 18.5.4);
- 5) (U) Interview or request information from the public or private entities (See DIOG Section 18.5.6);
(U//FOUO) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview.
- 6) (U) Information voluntarily provided by governmental or private entities (See DIOG Section 18.5.7); and
- 7) (U) Any other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

12.3.2.2.1.2 (U) PUBLIC HEALTH AND SAFETY AUTHORITIES IN RELATION TO DEMONSTRATIONS

- A) (U) At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety and to protect the exercise of First Amendment rights, such as:
- 1) (U) The time, place, and type of activities planned;
 - 2) (U) The number of persons expected to participate;
 - 3) (U) The expected means and routes of travel for participants and expected time of arrival; and
 - 4) (U) Any plans for lodging or housing of participants in connection with the demonstration.
- B) (U) The only investigative methods that may be used in an investigation under this paragraph are:
- 1) (U) Public Information (See DIOG Section 18.5.1);
 - 2) (U) Records or information – FBI and DOJ (See DIOG Section 18.5.2);
 - 3) (U) Records or information – other Federal, state, local, tribal, or foreign government agencies (See DIOG Section 18.5.3);
 - 4) (U) Use online services and resources (See DIOG Section 18.5.4);
 - 5) (U) Interview or request information from the public or private entities (See DIOG Section 18.5.6);
(U//FOUO) *Note:* Such interviews may only be conducted if the FBI employee identifies himself or herself as an FBI employee and accurately discloses the purpose of the interview;

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- 6) (U) Accept information voluntarily provided by governmental or private entities (See DIOG Section 18.5.7); and
- 7) (U) Any other methods may be used only if authorized by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division.

12.3.2.2.2 (U) APPROVAL REQUIREMENTS

- A) (U//FOUO) **General:** If assistance to another federal agency will involve the use of investigative methods other than those authorized for Assessments, prior Supervisory Special Agent (SSA) approval must be obtained with the FD-999. Supervisory approval for use of investigative methods authorized only for use during Predicated Investigations shall be at the same level required for use of that investigative method during an FBI investigation as provided in DIOG Sections 18.6 and 18.7. Approval for use of specific technologies is set forth in Section 12.4 below.
- B) (U//FOUO) **Sensitive Investigative Matters (SIM):** Any investigative assistance to other federal agencies involving a SIM requires prior CDC/OGC review and SAC/SC approval, and notification, as specified in 12.3.2.2.3.B below.

12.3.2.2.3 (U) NOTICE REQUIREMENTS

- A) (U//FOUO) **General:** Notice must be provided for the investigative activity or investigative method as specified in the DIOG and applicable MOU/MOAs.
- B) (U//FOUO) **Sensitive Investigative Matters (SIM):** In addition to the above-required approvals, any investigative assistance to another federal agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.
- C) (U//FOUO) **Classified Appendix:** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.2.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) to other Federal agencies using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3 (U) INVESTIGATIVE ASSISTANCE TO STATE, LOCAL AND TRIBAL AGENCIES

(U) The FBI may provide investigative assistance to state, local and tribal agencies:

- A) (U) in the investigation of crimes under state or local law when authorized by federal law (e.g., 28 U.S.C. §§ 540—felonious killing of state and local law enforcement officer; 540A—violent crime against travelers; 540B—serial killings);
- B) (U) in the investigation of matters that may involve federal crimes or threats to national security, or for such other purposes as may be legally authorized;

- C) (U) when such assistance is requested by the governor of the state pursuant to 42 U.S.C. § 10501 (for example, federal law enforcement assistance following Hurricane Katrina). The Attorney General must approve any request for assistance under 42 U.S.C. § 10501; and
- D) (U) under limited circumstances, the FBI is authorized to provide “expert” personnel to assist law enforcement agencies in their investigations. This authority is a limited exception to the general rule that the FBI cannot provide investigative assistance to investigate state crimes if there is no federal nexus.

(U) The authority to provide “expert assistance” to state investigations has been the subject of several opinions from the Office of Legal Counsel (OLC), DOJ. OLC has opined that the limited authority the FBI has in this area generally derives from its authority to “assist in conducting, at the request of a State [or] unit of local government... local and regional training programs for the training of State and local criminal justice personnel engaged in the investigation of crime and the apprehension of criminals,” 42 U.S.C. §3771, and its authority to provide Laboratory assistance even if there is no federal crime, 28 C.F.R. §0.85(g). OLC has made clear that this is not a broad grant of authority but instead is limited to assistance in circumstances where lives are in danger or there is a risk of serious bodily harm to a third person or a law enforcement officer. Adherence to the limitations set forth in this policy is important, as an employee whose actions exceed these limitations could be (a) acting beyond his or her official authority and therefore not entitled to qualified immunity from civil lawsuits or (b) acting outside the scope of his or her employment and therefore not entitled to DOJ representation if sued civilly.

(U) It should be stressed that the limitations on this authority relate to providing expert investigative assistance – not to other types of interaction that could be helpful to our domestic law enforcement colleagues, including standard liaison and training. Thus, for example, while it would not be permissible for the FBI to provide expert assistance to a state white collar investigation that has no federal nexus (because there is no life/safety concern), in the face of a request for such assistance, the ADIC/SAC of a field office could offer to have an experienced white collar investigator provide white collar investigative training to the police officers in lieu of providing investigative assistance.

(U) As used here, “expert personnel” are FBI employees who possess special skill or knowledge not normally possessed by professional law enforcement officers, that is derived from the employee’s education, training, or experience; the term does not include FBI employees who have specific knowledge about a particular investigation derived from participating in an investigation prior to the cessation of a federal nexus or otherwise.

(U) Areas of expertise for which requests for investigative assistance are commonly made include: Language Services, Polygraphers, Crisis Negotiators, Evidence Response Team (ERT), Special Weapons and Tactics (SWAT), Hostage Rescue Team (HRT), and Crisis Management. If the pertinent program has a PG or Policy Directive, the policy, procedures and approval requirements contained within the PG or Policy Directive must be followed.

12.3.2.3.1 (U) APPROVAL REQUIREMENTS

- A) (U) **General:** If the request for investigative assistance is based on Section 12.3.2.3. A or B above, the approval requirements specified in DIOG Sections 6 or 7 must be followed. If the request for investigative assistance is based on Section 12.3.2.3.C above, the Attorney General must approve the request.
- B) (U) **Expert Investigative Assistance:** If the request for expert investigative assistance is based on Section 12.3.2.3.D above and it is not covered by an existing PG or Policy Directive, the

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

ADIC/SAC in the field office (or the FBIHQ SC if the request is received at FBIHQ) may approve the request with notification as soon as practicable to the General Counsel if:

- 1) (U) The head (or designee) of the state, local, or tribal law enforcement agency has submitted a written request (including by email) to the FBI which:
 - a) (U) Identifies the need for specific expertise from the FBI;
 - b) (U) Articulates the risk of an imminent threat of death or serious injury to members of the public or law enforcement personnel or a significant risk to public safety; and
 - c) (U) Represents that the agency does not have available employees with the needed expertise or that the employees who do have the needed expertise are not sufficiently well trained to handle the immediate situation.
- (U) *Note:* If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally, but must be followed by a written request as soon as practicable, but not more than five (5) business days.
- 2) (U) The CDC, who is encouraged to consult with attorneys in the Investigative Law Unit, OGC (ILU), has reviewed the request and concluded that providing the requested assistance is consistent with this policy and does not create a significant risk of civil liability to the FBI or the individual employee. If the CDC assesses that the assistance will create a substantial risk of civil liability, the CDC must consult with ILU prior to approving the request. Additionally, the CDC is encouraged to consult with the Science and Technology Law Office (STLO) in OGC whenever questions arise concerning expert assistance associated with the use of Law Enforcement Sensitive (LES) technology, including techniques and capabilities.
 - 3) (U) The requesting agency is acting in the lawful execution of an authorized function of that organization; and
 - 4) (U) The loan of FBI personnel is an appropriate use of personnel and financial resources and does not jeopardize any ongoing FBI investigation.

12.3.2.3.2 (U) NOTICE REQUIREMENTS

- A) (U//FOUO) **General:** Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.
 - B) (U//FOUO) **Sensitive Investigative Matters (SIM):** In addition to the above-required approvals, any investigative assistance provided to a state, local, or tribal law enforcement agency involving a SIM requires notification to the appropriate FBIHQ operational unit and section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a sensitive investigative matter.
- (U//FOUO) **Classified Appendix:** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.3.2.3.3 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) Investigative assistance (including expert) using an investigative method, other than those authorized in assessments, must be documented with the FD-999, filed

and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below. Division PGs may require specific additional reporting requirements for their programs.

12.3.2.3.4 (U) EXAMPLES OF EXPERT INVESTIGATIVE ASSISTANCE

(U//FOUO) **Example 1:** A small town has experienced a string of muggings, but none of the victims, all elderly women, have been able to identify her attacker. The muggings have all occurred during commuting hours near shops. The community is quite upset. The local newspaper has published a number of stories on the attacks and reported that many women are afraid to leave their homes. The local police department is convinced that people have information that would help identify the assailant, but because the attacks take place during commuting hours they do not have enough officers to cover all the places where muggings have occurred during the short time frame of the attacks. They ask agents in the local RA to assist with interviewing commuters.

(U//FOUO) **Response 1:** The FBI cannot provide this assistance because this is a request to provide routine investigative assistance (additional manpower), not expert assistance.

(U//FOUO) **Example 2:** A midsize city police department receives several 911 calls indicating at least one, and perhaps more, gunmen have entered a 25-story office building and shot several employees on the 15th floor. One gunman was seen exiting the building, was chased by local police to a nearby home, and the gunman now holds several hostages and is shooting at police. The city's SWAT team deployed to the house. The local Police Chief orally requests for the assistance of the FBI's SWAT team and crisis negotiators because the department's SWAT personnel cannot cover both the house and the building simultaneously and the department does not have crisis negotiators.

(U//FOUO) **Response 2:** The SAC may provide this expert investigative assistance, notwithstanding the apparent lack of federal nexus, if local resources are insufficient to handle this emergency situation that poses an imminent risk of harm to the public. It would be appropriate for the FBI SWAT personnel to sweep the office building while local forces continue to deal with the barricaded subject. The crisis negotiators could be dispatched to the barricaded subject because the local department lacks such expertise. A crisis negotiator could also be deployed if the local police department had a crisis negotiator but assessed his/her skills were inadequate for the situation. Before granting the request, the SAC must have the CDC review it to determine whether there is a significant risk of civil liability. If the expert investigative assistance is provided, the field office must notify the General Counsel as soon as practicable. In addition, the oral request must be followed by a written request from the police department head as soon as practicable, but not more than five (5) business days. The investigative assistance rendered in these circumstances must be documented with the FD-999 and uploaded to the appropriate file as set forth in Section 12.5.

(U//FOUO) **Example 3:** A local police department is investigating a local doctor for molesting his pediatric patients. One of the potential victims is a 10 year old girl who is mentally disabled. The local FBI field office has a child victim expert who has expertise in interviewing mentally disabled children; the police department has a child victim specialist who has no specialized training in handling mentally disabled victims. The police chief seeks the assistance of the FBI's child victim specialist.

(U//FOUO) **Response 3:** The FBI may provide this requested assistance. Although there is no federal nexus, the FBI child victim specialist has relevant expertise that is not generally held within the law enforcement community and is not possessed by the local child victim specialist. The chief of police can articulate a risk of serious physical harm because until the

police can arrest the doctor, other children remain at risk of being molested. Before granting the request, the SAC must have the CDC review it to determine whether there is a significant risk of civil liability. If the expert investigative assistance is provided, the field office must notify the General Counsel as soon as practicable. The investigative assistance rendered in these circumstances must be documented with the FD-999 and uploaded to the appropriate file as set forth in Section 12.5.

12.3.2.4 (U) INVESTIGATIVE ASSISTANCE TO FOREIGN AGENCIES

(U//FOUO) The foundation of the FBI's international program is the Legal Attaché (Legat). Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and foreign investigative needs. The Legat can accomplish this because he/she develops partnerships and fosters cooperation with his or her foreign counterparts on every level and is familiar with investigative rules, protocols, and practices that differ from country to country. This is the Legat's primary responsibility. As such, foreign agency requests for assistance will likely come to the FBI through the Legat or International Operations Division (IOD). If, however, a foreign agency request for assistance bypasses the Legat or IOD and is received directly by the field office or FBIHQ division, the employee must obtain the prior approval of the IOD on the FD-999 before such assistance can be given, as discussed in this section.

12.3.2.4.1 (U) AUTHORITIES

- A) (U//FOUO) At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any US person (USPER). (AGG-Dom, Part III.D.1) The FBI must follow applicable MOUs and MOAs (to include those with other US Government (USG) agencies), Mutual Legal Assistance Treaties (MLAT), Letters Rogatory, and other treaties when it provides assistance to foreign governments.
- 1) (U//FOUO) If a request for foreign assistance is received directly from a foreign law enforcement or intelligence service and is not processed through a Legat or IOD, special approvals are required prior to providing the assistance, as specified in 12.3.2.4.2.B below.
- 2) (U//FOUO) The appropriate Legat must coordinate all requests for assistance from agencies within his/her area of responsibility to avoid duplicative requests and to ensure an FBI field office does not respond to a foreign request previously denied by the Legat or IOD.
- B) (U//FOUO) If a USAO requests FBI assistance pursuant to an MLAT, Letters Rogatory or other treaty request, the field office must open a foreign police cooperation file to document the assistance with written notification by LC or the FD-999 to the appropriate Legat and IOD.
- C) (U//FOUO) The FBI may not provide assistance to a foreign law enforcement, intelligence, or security officer conducting an investigation within the United States unless such officer has provided prior written notification to the Attorney General of his/her status as an agent of a foreign government, as required by 18 U.S.C. § 951. (AGG-Dom, Part III.D.2) The notification required by 18 U.S.C. § 951 is not applicable to diplomats, consular officers or attachés.

- D) (U//FOUO) Upon the request of a foreign government agency, the FBI may conduct background inquiries concerning individuals whose consent is documented. (AGG-Dom, Part III.D.3)

12.3.2.4.2 (U) APPROVAL REQUIREMENTS

- A) (U//FOUO) When a request to assist a foreign agency is received from a Legat or IOD, and such assistance will require the use of investigative methods other than those that are authorized in Assessments, prior SSA approval must be obtained and documented as specified in 12.3.2.4.4 below.
- B) (U//FOUO) If a request for assistance is received directly from a foreign law enforcement or intelligence service and is not processed through a Legat or IOD, written notification documenting the foreign assistance request must be provided to the appropriate Legat and IOD by the FD-999, and IOD must grant approval prior to providing assistance, regardless of what investigative methods are used. (See also classified provisions in DIOG Appendix G)
- C) (U//FOUO) The Office of International Affairs (OIA) in the DOJ's Criminal Division, has the responsibility and authority for the execution of all foreign assistance requests requiring judicial action or compulsory process. FBI IOD must coordinate all such requests with the DOJ OIA. (See DAG Memorandum, dated 5/16/2011, titled "Execution of Foreign Requests for Assistance in Criminal Cases.")
- D) (U//FOUO) Higher supervisory approvals and specific notifications may be required for assistance to foreign agencies involving joint operations, SIMs, and using particular investigative methods, as noted below and in Sections 10 and 18 of the DIOG, and in division PGs.
- E) (U//FOUO) Investigations and assistance conducted overseas, as well as related or official foreign travel of FBI personnel, require country clearances and notification to the Chief of Mission (COM) or designee. Such overseas investigations and assistance must adhere to the supplemental guidance in the IOD PG.

12.3.2.4.3 (U) NOTICE REQUIREMENTS

- A) (U//FOUO) When a foreign assistance request is submitted directly to a Legat or IOD by a foreign agency or through an FBIHQ-authorized joint task force operation involving foreign agencies that has previously been briefed to the Legat, IOD has notice of the request and the FBI employee does not need IOD approval prior to providing the assistance. The FBI employee must provide IOD and the Legat the results of the assistance.
- B) (U) The FBI must notify the DOJ NSD concerning investigation or assistance when: (i) FBIHQ's approval for the activity is required (e.g., FBIHQ approval is required to use a particular investigative method); and (ii) the activity relates to a threat to the United States national security. The FBIHQ division approving the use of the investigative method must notify DOJ NSD as soon as practicable, but no later than 30 calendar days after FBIHQ approval (see classified appendix for additional notice requirements). (AGG-Dom, Part III.D.1)
- C) (U//FOUO) Classified Appendix: See the classified provisions in DIOG Appendix G for additional notice requirements.
- D) (U//FOUO) Sensitive Investigative Matters (SIM): Any request for investigative assistance to a foreign agency involving a SIM requires OGC review and IOD SC approval, and notification as specified below. In addition to these approvals, any investigative assistance to a

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§12

foreign agency involving a SIM requires notification to the appropriate FBIHQ operational UC and SC by EC with an LHM suitable for dissemination to DOJ as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. Additionally, the appropriate IOD unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.

12.3.2.4.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) All investigative assistance to foreign agencies must be documented with an FD-999 and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below.

12.3.2.4.5 (U) EXAMPLES

(U//FOUO) **Example 1:** The local Australian Liaison Officer submits a request directly to his/her contact agent at the local FBI field office to run record checks (investigative assistance) on Platypus, Inc., an Australian-based company suspected of illegally exporting technology to China in violation of Australian law. The agent obtains SSA approval to run the records checks and completes an FD-999, which electronically notifies Legat Canberra and IOD of the request. Subsequently, the Legat approves the request, and the agent runs the record checks and gets negative results. The agent submits a summary EC documenting the Assessment request, SSA and Legat approvals, and the results are documented in a zero sub-assessment file with a "Read and Clear" lead to Legat Canberra and IOD.

(U//FOUO) **Example 2:** The same scenario as above, except the record checks provides a local address for a subsidiary of Platypus, Inc. In coordination with the Australian Liaison Officer, and with the approval of the SSA and IOD, the agent interviews an employee of the subsidiary and obtains statements incriminating Platypus, Inc. There does not appear to be a threat to the United States national security. The Australian Liaison Officer requests the employee be polygraphed (expert assistance). The agent obtains SSA approval to conduct the polygraph examination (because it is a method not permitted during an Assessment and SSA approval is required in DIOG Section 18.6.12 for the use of this investigative method) and documents the request and approval in the FD-999. Upon completion of the assistance, the results are documented in the appropriate file with a "Read and Clear" lead to Legat Canberra and IOD.

12.4 (U) TECHNICAL ASSISTANCE TO OTHER AGENCIES – STANDARDS, APPROVALS AND NOTICE REQUIREMENTS

(U//FOUO) FBI technical assistance may be provided to other agencies when:

- A) (U//FOUO) the technical assistance is within the scope authorized by the AGG-Dom, Federal laws, regulations, or other legal authorities;
- B) (U//FOUO) the technical assistance is being provided in connection with a matter that is not based solely on the exercise of First Amendment activities or on the race, ethnicity, national origin or religion of the subject or a combination of only these factors; and
- C) (U//FOUO) the technical assistance is an appropriate use of FBI personnel and financial resources.

12.4.1 (U) AUTHORITY

(U//FOUO) Pursuant to 28 C.F.R. §0.85(g), FBI Laboratories, including but not limited to, the Laboratory Division, Operational Technology Division's Digital Evidence Laboratory, and Regional Computer Forensic Laboratories are authorized to provide technical or scientific assistance and expert testimony to any duly constituted law enforcement agency. Additionally, pursuant to Attorney General (AG) Order 2954-2008, the FBI is authorized to provide reasonable technical and expert assistance to Federal, state, local, and tribal law enforcement agencies to assist such agencies in the lawful execution of their authorized functions. (See also 28 U.S.C §§ 509, 510 and 530(C)). Such assistance may also be provided to certain foreign agencies (see Section 12.4.2.4 below). Under the Order, such technical and expert assistance includes, but is not limited to:

- A) (U) Lending or sharing equipment or property;
- B) (U) Sharing facilities or services;
- C) (U) Collaborating in the development, manufacture, production, maintenance, improvement, distribution, or protection of technical investigative capabilities;
- D) (U) Sharing or providing transmission, switching, processing, storage or other services;
- E) (U) Disclosing technical designs, knowledge, information or expertise, or providing training in the same;
- F) (U) Providing the assistance of expert personnel in accordance with written guidelines issued by the FBI General Counsel or approved by the General Counsel (See Section 12.3.2.3 above); and
- G) (U) Providing forensic analysis and examination of submitted evidence.

12.4.2 (U) APPROVAL REQUIREMENTS

12.4.2.1 (U) TECHNICAL ASSISTANCE TO USIC AGENCIES

(U//FOUO) Before providing technical assistance to a USIC agency, the appropriate FBIHQ operational division as well as the OTD should be consulted to determine whether such assistance is governed by an existing PG, MOU or other agreement.

12.4.2.2 (U) TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL AND TRIBAL (DOMESTIC) AGENCIES REGARDING ELECTRONIC SURVEILLANCE, EQUIPMENT, AND FACILITIES

(U) Field-based technical assistance requests under this section must be approved by the field office Assistant Director in Charge (ADIC) or SAC in compliance with the Operational Technology Division (OTD) Domestic Technical Assistance (DTA) PG. If the request for technical assistance involves equipment, facilities or property from more than one field office, each field office must approve the use of its resources.

(U) As specified below, FBIHQ senior executive officials and/or officials of the DOJ must approve a request for FBI technical assistance that involves:

- A) (U) Sensitive Circumstances, as defined in DIOG Section 18.7.2.6., where approval is required by an FBIHQ senior executive official or DOJ official designated therein;

- B) (U) Use of National Security Classified Investigative Technologies in criminal investigations, where approval is required by the Deputy Attorney General, DOJ. The request should be submitted for processing to the appropriate FBIHQ operational division unit responsible for the investigation and to the OTD SC with program responsibility;
- C) (U) Surreptitious (non-consensual) entry into a premises or vehicle or other technical operations determined by the Technical Advisor to present a similar risk. Such requests require the joint approval of the OTD SC with programmatic responsibility for tactical (covert entry) operations and the field office SAC or ADIC; or
- D) (U) Assistance to foreign law enforcement agencies (See Section 12.4.2.4 below).

(U) The OTD Foreign Technical Assistance (FTA) PG provides additional details specifying the procedures and approval process that must be followed when the FBI is providing technical assistance regarding electronic surveillance, equipment, and facilities.

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 and the OTD FTA PG.

12.4.2.3 (U) TECHNICAL ASSISTANCE TO FEDERAL, STATE, LOCAL AND TRIBAL (DOMESTIC) AGENCIES INVOLVING EQUIPMENT OR TECHNOLOGIES OTHER THAN ELECTRONIC SURVEILLANCE EQUIPMENT

(U) There are limited other situations in which, in the absence of a federal nexus, a domestic law enforcement agency may seek technical assistance through the short term loan of equipment from the FBI. If there is an applicable PG or Policy Directive, the policy and procedures contained within the PG or Policy Directive must be followed (see, e.g., Corporate Policy Directive: Deployment of MRAP Armored Vehicles in the Absence of Federal Jurisdiction). If no PG or Policy Directive governs the particular equipment sought to be borrowed *and* if the loan of the equipment does not necessarily also entail the loan of personnel to use or operate the equipment, then the ADIC/SAC of the field office must approve the loan of the equipment in accordance with the following policy and procedures. If the loan of the equipment necessarily entails the loan of FBI employees, the policies governing expert assistance set forth below must also be followed.

(U) Any loan of equipment must be documented through a written agreement between the ADIC/SAC and the head of the borrowing law enforcement agency or his/her designee. At a minimum, the agreement must provide that the borrowing law enforcement agency will reimburse the FBI should the equipment be lost or damaged and that the borrowing law enforcement agency will promptly return the equipment when asked to do so by the FBI. If due to the exigency of the situation there is not time for the request to be submitted in writing, the request may be made orally but must be followed by a written agreement as soon as practicable, but not more than five (5) business days following the loan.

(U) In considering whether to lend the equipment to the federal, state, local and tribal law enforcement agency, the ADIC/SAC must take into account the following:

- A) (U) The purpose for which the equipment is being requested and how the equipment will be used to advance that objective;
- B) (U) The likelihood that the equipment will be damaged by the requested use;

- C) (U) The likelihood that the field office will need the equipment during the proposed loan period; and
- D) (U) Whether the borrowing law enforcement agency has previously violated the terms of any loan of equipment or damaged any equipment previously lent by the FBI.

(U) The OTD FTA PG provides additional details specifying the procedures and approval process that must be followed when the FBI is providing equipment or technologies other than electronic surveillance equipment.

(U) For technical assistance to foreign law enforcement agencies see Section 12.4.2.4 below and the OTD Foreign Technical Assistance (FTA) PG.

12.4.2.4 (U) TECHNICAL ASSISTANCE TO FOREIGN AGENCIES

12.4.2.4.1 (U) AUTHORITIES

- A) (U//FOUO) The AGG-Dom, Part III.D.4 authorizes the FBI to provide other technical assistance to foreign governments to the extent not otherwise prohibited by law.
- B) (U//FOUO) AG Order 2954-2008 authorizes the FBI to provide technical assistance to foreign national security and law enforcement agencies cooperating with the FBI in the execution of the FBI's counter-terrorism and counter-intelligence duties and to foreign law enforcement agencies to assist such agencies in the lawful execution of their authorized functions. Requests under this section for technical assistance with respect to electronic surveillance and other OTD technologies are to be handled pursuant to the OTD FTA PG.

12.4.2.4.2 (U) APPROVAL REQUIREMENTS

(U//FOUO) Approvals of requests for technical assistance to foreign agencies are to be handled pursuant to the OTD FTA PG.

12.4.2.4.3 (U) NOTICE REQUIREMENTS

- A) (U//FOUO) **General:** Notice must be provided for the investigative activity or investigative method as specified in the DIOG, and applicable MOU/MOAs and/or treaties.
- B) (U//FOUO) **Sensitive Investigative Matters (SIM):** In addition to the above-required approvals, any investigative technical assistance to the agencies listed in this section involving a SIM requires approval by the SAC (HQ assistance requires SC approval) with notification to the appropriate FBIHQ operational unit and section and appropriate OTD section by EC as soon as practicable, but no later than 15 calendar days after the initiation of the assistance. The appropriate FBIHQ operational unit must provide notice to the DOJ Criminal Division or NSD as soon as practicable, but not later than 30 calendar days after the initiation of any assistance involving a SIM.
- C) (U//FOUO) **Classified Appendix:** See the classified provisions in DIOG Appendix G for additional notice requirements.

12.4.2.4.4 (U) DOCUMENTATION REQUIREMENTS

(U//FOUO) All technical assistance rendered must be documented with the FD-999, filed and uploaded to an appropriate file as specified in Sections 12.5 and 12.6 below.

12.5 (U) DOCUMENTATION REQUIREMENTS FOR INVESTIGATIVE OR TECHNICAL ASSISTANCE TO OTHER AGENCIES

12.5.1 (U) DOCUMENTATION REQUIREMENTS IN GENERAL

(U//FOUO) When required by this section, the FD-999 must be used to document assistance to other agencies (domestic or foreign) or the dissemination of information. The FD-999 must be completed by the FBI division, field office, or Legat that provides the assistance or disseminates the information. (For example, if an FBIHQ division receives a request for assistance from another federal agency and forwards the request to the field office that can provide the assistance, that field office is required to complete the FD-999.)

(U//FOUO) When an FD-999 is used to document the “dissemination” of information to another agency, it is understood that “assistance” was provided to said agency and a separate FD-999 does not have to be completed to document the assistance to that agency (domestic or foreign).

12.5.2 (U) DOCUMENTATION REQUIREMENTS FOR INVESTIGATIVE ASSISTANCE (INCLUDING EXPERT ASSISTANCE) TO OTHER AGENCIES (DOMESTIC OR FOREIGN)

(U//FOUO) **Mandatory use of the FD-999:** The FD-999 must be used when providing investigative assistance, including expert investigative assistance, using an investigative method other than those authorized in Assessments to:

- A) (U) USIC Agencies;
- B) (U) United States Federal Agencies;
- C) (U) State, Local, or Tribal Agencies; or
- D) (U) Foreign Agencies.

(U//FOUO) **Exception:** Regardless of investigative methods used, if a request for foreign investigative assistance is received directly from a foreign law enforcement or intelligence service and is not processed through a Legat or IOD, written notification documenting the foreign investigative assistance request must be provided to the appropriate Legat and IOD by the FD-999, and IOD must grant approval prior to providing the assistance.

(U//FOUO) **Example:** Another federal agency requests the FBI to participate in an interview. The FBI does not have an open investigation in the matter. In such circumstances, it is not necessary to complete an FD-999 to document the assistance because the investigative method (interview) is authorized for use in Assessments and does not require supervisory approvals or documentation. However, if the FD-302 will be disseminated to the requesting federal agency then an FD-999 must be prepared.

12.5.3 (U) DOCUMENTATION REQUIREMENTS FOR TECHNICAL ASSISTANCE TO OTHER AGENCIES (DOMESTIC OR FOREIGN)

(U//FOUO) **Mandatory use of the FD-999:** The FD-999 must be used when providing any technical assistance to:

- A) (U) USIC Agencies;
- B) (U) United States Federal Agencies;
- C) (U) State, Local, or Tribal Agencies; or
- D) (U) Foreign Agencies.

12.6 (U) DISSEMINATION OF INFORMATION TO OTHER AGENCIES – DOCUMENTATION REQUIREMENTS

(U//FOUO) Dissemination of information to other agencies must be consistent with Director of National Intelligence directives, the AGG-Dom, DIOG Section 14, FBI Foreign Dissemination Manual, the Privacy Act of 1974, and any applicable MOU/MOA, law, treaty or other policy.

(U//FOUO) Classified information may only be disseminated pursuant to applicable federal law, Presidential directive, Attorney General policy and FBI policy.

(U) The Privacy Act mandates specific documentation of any dissemination of information to an agency outside the DOJ involving a U.S. Citizen or alien lawfully admitted for permanent residence, i.e., a U.S. person (USPER).

(U//FOUO) Dissemination of information to foreign agencies must be in accordance with the FBI Foreign Dissemination Manual, dated May 23, 2008, or as revised.

(U//FOUO) **Mandatory use of the FD-999:** The FD-999 must be used to document the dissemination of all unclassified or classified (up to Secret level) information to:

- A) (U) USIC Agencies;
- B) (U) United States Federal Agencies - when the disseminated information is related to their respective responsibilities;
- C) (U) State, Local, or Tribal Agencies - when the disseminated information is related to their respective responsibilities; or
- D) (U) Foreign Agencies.

(U//FOUO) **Note:** Dissemination of Top Secret or higher classified information must be documented in the appropriate classified file or the Sensitive Compartmented Information Operational Network (SCION).

(U//FOUO) **Optional use of the FD-999:** The FD-999 is permitted, but is not required to be used, for the dissemination of information if:

- A) (U//FOUO) the information disseminated is being furnished to an agency within the DOJ with which the FBI is working a joint investigation; or

- B) (U//FOUO) the information is disseminated with an IIR, SIR, or other FBI document that is maintained in an approved database of records.

12.7 (U) RECORDS RETENTION REQUIREMENTS

12.7.1 (U) USE OF THE FD-999

(U//FOUO) All FD-999s must be created on the FBI's SharePoint site. This requirement allows the FBI to maintain a database to comply with the AGG-Dom, Part III.E.3 because it will permit, with respect to each such activity, the prompt retrieval of the:

- A) (U) status of the assistance activity (opened or closed);
- B) (U) the dates of opening and closing; and
- C) (U) the basis for the assistance activity.

12.7.2 (U) UPLOADING THE FD-999

(U//FOUO) The FD-999 must be uploaded to the appropriate file, which may be:

- A) (U) an Assessment file;
- B) (U) a zero sub-assessment file;
- C) (U) a Predicated Investigation file;
- D) (U) a domestic police cooperation file – 343 Classification (the new 343 file classification system replaces the former 62 classification) as described below;
- E) (U) a foreign police cooperation file – 163 Classification (the revised 163 file classification system) as described below;
- F) (U) a zero classification file; or
- G) (U) any other investigative or technical assistance control file using a unique investigative file number created by the field office, Legat, or FBIHQ division to document the dissemination of information or assistance to another agency.

(U//FOUO) These records will assume the NARA approved retention periods approved for the file classification in which they are maintained.

12.7.3 (U) REQUEST FOR FD-999 EXEMPTION

(U//FOUO) FBI entities/programs may submit to the Corporate Policy Office (CPO), Director's Office, a written request for an exemption to the mandatory FD-999 requirements contained in DIOG Section 12 provided the entity/program maintains a similar database to permit the prompt retrieval of the information required above. The CPO, in conjunction with personnel from the Office of Integrity and Compliance (OIC) and the OGC, will evaluate the exemption request to determine database compliance with the AGG-Dom. The CPO will approve or deny the exemption request, and maintain a list of all approved exempted entities/programs.

12.7.4 (U//FOUO) 343 FILE CLASSIFICATION - DOMESTIC POLICE COOPERATION FILES

(U//FOUO) The former 62 file classification may no longer be utilized to document domestic police cooperation. The new **343** file classification system with alpha-designators must be utilized to document domestic police cooperation matters.

12.7.5 (U//FOUO) 163 FILE CLASSIFICATION – FOREIGN POLICE COOPERATION FILES

(U//FOUO) The 163 file classification was revised with “new” alpha-designators. The 163 file classification system must be utilized to document foreign police cooperation matters.

13 (U) EXTRATERRITORIAL PROVISIONS

13.1 (U) OVERVIEW

(U//FOUO) The FBI may conduct investigations abroad, participate with foreign officials in investigations abroad, or otherwise conduct activities outside the United States. The guidelines for conducting investigative activities outside of the United States are currently contained in:

- A) (U) *The Attorney General's Guidelines for Extraterritorial FBI Operations and Criminal Investigations*;
- B) (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG, Part II.E)*;
- C) (U) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions*;
- D) (U) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and
- E) (U) *Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation* (2005).

(U//FOUO) Collectively, these guidelines and procedures are referred to in the DIOG as the Extraterritorial Guidelines.

13.2 (U) PURPOSE AND SCOPE

(U//FOUO) As a general rule, the Extraterritorial Guidelines apply when FBI personnel or confidential human sources (CHS) are actively engaged in investigative activity outside the borders of the United States. In addition, investigative activities that may be undertaken in the United States but that have an intrusive effect on the domestic affairs of a foreign country and may be considered by the governing authorities of that country to constitute an invasion of its sovereignty are governed by the Extraterritorial Guidelines. The following is a list of such activities:

- A) (U//FOUO) Opening a bank account in a foreign financial institution from the United States for the purpose of laundering money;
- B) (U//FOUO) Causing or facilitating the transportation of stolen or counterfeit property into or through another country;
- C) (U//FOUO) Causing or facilitating the transportation of narcotics into or through another country;
- D) (U//FOUO) Conducting a non-consensual search of a known foreign-based computer;
- E) (U//FOUO) Breaching the security of a known foreign-based computer security system;
- F) (U//FOUO) Opening an undercover business in another country from the United States;

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§13

- G) (U//FOUO) Applying for a permit or license or otherwise making use of another country's government facilities, institutions or processes using a covert identity;
- H) (U//FOUO) Facilitating a person's unlawful entry into another country by creating false documentation;
- I) (U//FOUO) Consensual monitoring of communications with a senior foreign government official involving the official's duties or misuse of his/her office; and
- J) (U//FOUO) Any other investigative activity that, although it is conducted from the United States, is likely to create the same level of intrusion as the activities listed above or, for other reasons, has the reasonable potential to adversely impact United States foreign relations.

(U//FOUO) FBI personnel planning to engage in any of the investigative activities described in the subsection above must obtain the concurrence of the appropriate Legal Attaché (Legat) and must comply with the remaining procedural requirement of the Extraterritorial Guidelines, which may be found in the classified provisions in DIOG Appendix G.

13.3 (U) JOINT VENTURE DOCTRINE

(U//FOUO) The "joint venture" doctrine provides that in certain circumstances, Fourth or Fifth Amendment rights may attach and evidence seized overseas, including statements of a defendant, may be subject to suppression if the foreign law enforcement officers did not comply with U.S. law. A determination that a "joint venture" exists requires a finding of "active" or "substantial" involvement by U.S. agents in the foreign law enforcement activity. Because the determination will be fact specific and very few cases illuminate what constitutes "active" or "substantial" participation, FBI employees should contact their CDC or OGC for guidance. See also Chapter 35, DOJ Federal Narcotics Manual (March 2011) available on the DOJ intranet.

13.4 (U) LEGAL ATTACHÉ PROGRAM

(U//FOUO) The foundation of the FBI's international program is the Legat. Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and extraterritorial investigative needs. Legats can accomplish this mission because they have developed partnerships and fostered cooperation with their foreign counterparts on every level and are familiar with local investigative rules, protocols, and practices which differ from country to country. For additional information consult the FBIHQ IOD website.

14 (U) RETENTION AND SHARING OF INFORMATION

14.1 (U) PURPOSE AND SCOPE

(U//FOUO) Every FBI component is responsible for the creation and maintenance of authentic, reliable, and trustworthy records. (Note: If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM, etc.) should reflect that another party, and not the FBI, is the originator of the characterization). Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, or perform any of its critical missions effectively.

(U//FOUO) The FBI is committed to ensuring that its records management program accomplishes the following goals:

- A) (U//FOUO) Facilitates the documentation of official decisions, policies, activities, and transactions;
- B) (U//FOUO) Facilitates the timely retrieval of needed information;
- C) (U//FOUO) Ensures continuity of FBI business;
- D) (U//FOUO) Controls the creation and growth of FBI records;
- E) (U//FOUO) Reduces operating costs by managing records according to FBI business needs and by disposing of unneeded records in a timely manner;
- F) (U//FOUO) Improves efficiency and productivity through effective records storage and retrieval methods;
- G) (U//FOUO) Ensures compliance with applicable laws and regulations;
- H) (U//FOUO) Safeguards the FBI's mission-critical information;
- I) (U//FOUO) Preserves the FBI's corporate memory and history; and
- J) (U//FOUO) Implements records management technologies to support all of the goals listed above.

(U) Note: The hardcopy file is the “**official file**” at the present time and a hardcopy of all electronic or on-line forms or documents must be printed and serialized into the field office or FBIHQ hardcopy file.

14.2 (U) THE FBI'S RECORDS RETENTION PLAN, AND DOCUMENTATION

(U//FOUO) The FBI must retain records relating to investigative activities according to the FBI's records retention plan that has been approved by the National Archives and Records Administration (NARA). (AGG-Dom, Part VI.A.1)

(U//FOUO) The FBI's disposition authorities provide specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§13

- G) (U//FOUO) Applying for a permit or license or otherwise making use of another country's government facilities, institutions or processes using a covert identity;
- H) (U//FOUO) Facilitating a person's unlawful entry into another country by creating false documentation;
- I) (U//FOUO) Consensual monitoring of communications with a senior foreign government official involving the official's duties or misuse of his/her office; and
- J) (U//FOUO) Any other investigative activity that, although it is conducted from the United States, is likely to create the same level of intrusion as the activities listed above or, for other reasons, has the reasonable potential to adversely impact United States foreign relations.

(U//FOUO) FBI personnel planning to engage in any of the investigative activities described in the subsection above must obtain the concurrence of the appropriate Legal Attaché (Legat) and must comply with the remaining procedural requirement of the Extraterritorial Guidelines, which may be found in the classified provisions in DIOG Appendix G.

13.3 (U) JOINT VENTURE DOCTRINE

(U//FOUO) The "joint venture" doctrine provides that in certain circumstances, Fourth or Fifth Amendment rights may attach and evidence seized overseas, including statements of a defendant, may be subject to suppression if the foreign law enforcement officers did not comply with U.S. law. A determination that a "joint venture" exists requires a finding of "active" or "substantial" involvement by U.S. agents in the foreign law enforcement activity. Because the determination will be fact specific and very few cases illuminate what constitutes "active" or "substantial" participation, FBI employees should contact their CDC or OGC for guidance. See also Chapter 35, DOJ Federal Narcotics Manual (March 2011) available on the DOJ intranet.

13.4 (U) LEGAL ATTACHÉ PROGRAM

(U//FOUO) The foundation of the FBI's international program is the Legat. Each Legat is the Director's personal representative in the foreign countries in which he/she resides or has regional responsibilities. The Legat's job is to respond to the FBI's domestic and extraterritorial investigative needs. Legats can accomplish this mission because they have developed partnerships and fostered cooperation with their foreign counterparts on every level and are familiar with local investigative rules, protocols, and practices which differ from country to country. For additional information consult the FBIHQ IOD website.

14 (U) RETENTION AND SHARING OF INFORMATION

14.1 (U) PURPOSE AND SCOPE

(U//FOUO) Every FBI component is responsible for the creation and maintenance of authentic, reliable, and trustworthy records. (Note: If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM, etc.) should reflect that another party, and not the FBI, is the originator of the characterization). Without complete and accessible records, the FBI cannot conduct investigations, gather and analyze intelligence, assist with the prosecution of criminals, or perform any of its critical missions effectively.

(U//FOUO) The FBI is committed to ensuring that its records management program accomplishes the following goals:

- A) (U//FOUO) Facilitates the documentation of official decisions, policies, activities, and transactions;
- B) (U//FOUO) Facilitates the timely retrieval of needed information;
- C) (U//FOUO) Ensures continuity of FBI business;
- D) (U//FOUO) Controls the creation and growth of FBI records;
- E) (U//FOUO) Reduces operating costs by managing records according to FBI business needs and by disposing of unneeded records in a timely manner;
- F) (U//FOUO) Improves efficiency and productivity through effective records storage and retrieval methods;
- G) (U//FOUO) Ensures compliance with applicable laws and regulations;
- H) (U//FOUO) Safeguards the FBI's mission-critical information;
- I) (U//FOUO) Preserves the FBI's corporate memory and history; and
- J) (U//FOUO) Implements records management technologies to support all of the goals listed above.

(U) Note: The hardcopy file is the “**official file**” at the present time and a hardcopy of all electronic or on-line forms or documents must be printed and serialized into the field office or FBIHQ hardcopy file.

14.2 (U) THE FBI'S RECORDS RETENTION PLAN, AND DOCUMENTATION

(U//FOUO) The FBI must retain records relating to investigative activities according to the FBI's records retention plan that has been approved by the National Archives and Records Administration (NARA). (AGG-Dom, Part VI.A.1)

(U//FOUO) The FBI's disposition authorities provide specific instructions about the length of time that records must be maintained. In some instances, records may be destroyed after a

prescribed period of time has elapsed. Other records are never destroyed and are transferred to NARA a certain number of years after an investigation is closed.

14.2.1 (U) DATABASE OR RECORDS SYSTEM

(U//FOUO) The FBI must maintain a database or records system that permits, with respect to each Predicated Investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation. (AGG-Dom, Part VI.A.2)

(U//FOUO) The FBI's official File Classification System covers records related to all investigative and intelligence collection activities, including Assessments. Records must be maintained in the FBI's Central Records System, or other designated systems of records, which provides the required maintenance and retrieval functionality.

14.2.2 (U) RECORDS MANAGEMENT DIVISION DISPOSITION PLAN AND RETENTION SCHEDULES

(U//FOUO) (U//FOUO) All investigative records, whether from Assessments or Predicated Investigations, must be retained in accordance with the Records Management Division Disposition Plan and Retention Schedules. No records, including those generated during Assessments, may be destroyed or expunged earlier than the destruction schedule without written approval from NARA, except in "expungement" circumstances as further described in RMD policy. Records, including those generated during Assessments, may not be retained longer than the destruction schedule unless otherwise directed by RMD to include, "litigation hold" circumstances as described in RMD policy. See the RMD webpage and [http://home.fbinet.fbi/DO/RMD/RPAS/RDU/Pages/RecordFreezes\(Holds\)LitigationFreezeList.aspx](http://home.fbinet.fbi/DO/RMD/RPAS/RDU/Pages/RecordFreezes(Holds)LitigationFreezeList.aspx). In the event an office believes they need to retain records beyond their destruction schedule, they should contact RMD for further guidance.

14.3 (U) INFORMATION SHARING

(U//FOUO) The FBI 2008 National Information Sharing Strategy (NISS) provides the common vision, goals, and framework needed to guide information sharing initiatives with our federal, state, local, and tribal agency partners, foreign government counterparts, and private sector stakeholders. The FBI NISS addresses the cultural and technological changes required to move the FBI to "a responsibility to provide" culture.

14.3.1 (U) PERMISSIVE SHARING

(U//FOUO) Consistent with the Privacy Act, FBI policy, and any other applicable laws and memoranda of understanding or agreement with other agencies concerning the dissemination of information, the FBI may disseminate information obtained or produced through activities under the AGG-Dom:

- A) (U//FOUO) Within the FBI and to all other components of the DOJ if the recipients need the information in the performance of their official duties.

- B) (U//FOUO) To other federal agencies if disclosure is compatible with the purpose for which the information was collected and it is related to their responsibilities. In relation to other USIC agencies, the determination whether the information is related to the recipient responsibilities may be left to the recipient.
- C) (U//FOUO) To state, local, or Indian tribal agencies directly engaged in the criminal justice process when access is directly related to a law enforcement function of the recipient agency.
- D) (U//FOUO) To Congress or to congressional committees in coordination with the FBI Office of Congressional Affairs (OCA) and the DOJ Office of Legislative Affairs.
- E) (U//FOUO) To foreign agencies if the FBI determines that the information is related to their responsibilities; the dissemination is consistent with the interests of the United States (including national security interests); consideration has been given to the effect on any identifiable USPER; and disclosure is compatible with the purpose for which the information was collected.
- F) (U//FOUO) If the information is publicly available, does not identify USPERs, or is disseminated with the consent of the person whom it concerns.
- G) (U//FOUO) If the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national security, or to obtain information for the conduct of an authorized FBI investigation.
- H) (U//FOUO) If dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. § 552a) (AGG-Dom, Part VI.B.1)

(U//FOUO) All FBI information sharing activities under this section shall be done in accordance with Corporate Policy Directive 12D, “FBI Sharing Activities with Other Government Agencies,” and Corporate Policy Directive 95D “Protecting Privacy in the Information Sharing Environment,” and any amendments thereto and applicable succeeding policy directives.

14.3.2 (U) REQUIRED SHARING

(U//FOUO) The FBI must share and disseminate information as required by law and applicable policy. Working through the supervisory chain and other appropriate entities, FBI employees must ensure compliance with statutes, including the Privacy Act, treaties, Executive Orders, Presidential directives, National Security Council (NSC) directives, Homeland Security Council (HSC) directives, Director of National Intelligence directives, Attorney General-approved policies, and MOUs or MOAs.

14.4 (U) INFORMATION RELATED TO CRIMINAL MATTERS

14.4.1 (U) COORDINATING WITH PROSECUTORS

(U//FOUO) In an investigation relating to possible criminal activity in violation of federal law, the FBI employee conducting the investigation must maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the FBI employee must present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed must be available on request to a United States Attorney (USA) or his or her designee or an appropriate DOJ official. (AGG-Dom, Part VI.C)

14.4.2 (U) CRIMINAL MATTERS OUTSIDE FBI JURISDICTION

(U//FOUO) When credible information is received by an FBI employee concerning serious criminal activity not within the FBI's investigative jurisdiction, the FBI employee must promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except when disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a CHS, interfere with the cooperation of a CHS, or reveal legally privileged information. If full disclosure is not made for any of the reasons indicated, then, whenever feasible, the FBI employee must make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure must be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI employee/field office must promptly notify FBIHQ in writing of the facts and circumstances concerning the criminal activity. The FBI must make periodic reports to the Deputy Attorney General of such non-disclosures and incomplete disclosures, in a form suitable to protect the identity of a CHS. (AGG-Dom, Part VI.C)

14.4.3 (U) REPORTING CRIMINAL ACTIVITY OF AN FBI EMPLOYEE OR CHS

(U//FOUO) When it appears that an FBI employee has engaged in criminal activity in the course of an investigation, the FBI must notify the USAO or an appropriate DOJ division. When it appears that a CHS has engaged in criminal activity in the course of an investigation, the FBI must proceed as provided in the AGG-CHS. When information concerning possible criminal activity by any other person appears in the course of an investigation, the FBI may open an investigation of the criminal activity if warranted, and must proceed as provided in Section 14.4.1 and 14.4.2 above. (AGG-Dom, Part VI.C.3)

(U//FOUO) The reporting requirements under this paragraph relating to criminal activity by an FBI employee or a CHS do not apply to otherwise illegal activity that is authorized in conformity with the AGG-Dom or other Attorney General guidelines or to minor traffic offenses. (AGG-Dom, Part VI.C.3)

14.5 (U) INFORMATION RELATED TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

(U//FOUO) All information sharing with a foreign government related to classified national security and foreign intelligence must be done in accordance with the FBI Foreign Dissemination Manual and effective policies governing MOUs.

(U//FOUO) The general principle reflected in current law and policy is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. The FBI's responsibility in this area includes carrying out the requirements of the MOU Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and

consultation with other DOJ components, and for sharing national security and foreign intelligence information with White House agencies, as provided below. (AGG-Dom, Part VI.D)

14.5.1 (U) DEPARTMENT OF JUSTICE

(U//FOUO) The DOJ National Security Division (NSD) must have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for NSD must consult concerning these activities whenever requested by either of them, and the FBI must provide such reports and information concerning these activities as the Assistant Attorney General for NSD may request. In addition to any reports or information the Assistant Attorney General for NSD may specially request under this subparagraph, the FBI must provide annual reports to the NSD concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office. (AGG-Dom, Part VI.D.1)

(U//FOUO) The FBI must keep the NSD apprised of all information obtained through activities under the AGG-Dom that is necessary to the ability of the United States to investigate or protect against threats to the national security; this should be accomplished with regular consultations between the FBI and the NSD to exchange advice and information relevant to addressing such threats through criminal prosecution or other means. (AGG-Dom, Part VI.D.1)

(U//FOUO) Except for counterintelligence investigations, a relevant USAO must have access to and must receive information from the FBI relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the NSD. The relevant USAO must receive such access and information from the FBI field offices. (AGG-Dom, Part VI.D.1)

(U//FOUO) In a counterintelligence investigation – i.e., an investigation of espionage or other intelligence activities, sabotage, or assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons [AGG-Dom, Part VII.S.2]– the FBI may only provide information to and consult with a relevant USAO if authorized to do so by the NSD. Until the policies required by AGG-Dom, Part VI.D.1.d are promulgated, the FBI may consult freely with the USAO concerning investigations within the scope of this subparagraph during an emergency, so long as the NSD is notified of such consultation as soon as practicable after the consultation. (AGG-Dom, Part VI.D.1).

(U//FOUO) Information shared with a USAO pursuant to DIOG Section 14.5 (National Security) must be disclosed only to the USA or any AUSA designated by the USA as points of contact to receive such information. The USA and designated AUSA must have an appropriate security clearance and must receive training in the handling of classified information and information derived from FISA, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information. (AGG-Dom, Part VI.D.1)

(U//FOUO) The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the FISC, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney

General in particular investigations. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of a CHS is governed by the relevant provisions of the AGG-CHS. (AGG-Dom, Part VI.D.1)

14.5.2 (U) THE WHITE HOUSE

(U//FOUO) In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the NSC and its staff, the HSC and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. Accordingly, the FBI may disseminate to the White House foreign intelligence and national security information obtained through activities under the AGG-Dom, subject to the following standards and procedures.

14.5.2.1 (U) REQUESTS SENT THROUGH NSC OR HSC

(U//FOUO) The White House must request such information through the NSC staff or HSC staff including, but not limited to, the NSC Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President. (AGG-Dom, Part VI.D.2.a)

(U//FOUO) If the White House sends a request for such information to the FBI without first sending the request through the entities described above, the request must be returned to the White House for resubmission.

14.5.2.2 (U) APPROVAL BY THE ATTORNEY GENERAL

(U//FOUO) Compromising information concerning domestic officials or domestic political organizations, or information concerning activities of USPERs intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. Such approval is not required, however, for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House or concerning contacts by White House personnel with foreign intelligence service personnel. (AGG-Dom, Part VI.D.2.b)

14.5.2.3 (U) INFORMATION SUITABLE FOR DISSEMINATION

(U//FOUO) Examples of the type of information that is suitable for dissemination to the White House on a routine basis includes, but is not limited to (AGG-Dom, Part VI.D.2.c):

- A) (U//FOUO) Information concerning international terrorism;
- B) (U//FOUO) Information concerning activities of foreign intelligence services in the United States;
- C) (U//FOUO) Information indicative of imminent hostilities involving any foreign power;
- D) (U//FOUO) Information concerning potential cyber threats to the United States or its allies;

- E) (U//FOUO) Information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
- F) (U//FOUO) Information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
- G) (U//FOUO) Information concerning foreign economic or foreign political matters that might have national security ramifications; and
- H) (U//FOUO) Information set forth in regularly published national intelligence requirements.

14.5.2.4 (U) NOTIFICATION OF COMMUNICATIONS

(U//FOUO) Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending investigation must be made known to the Office of the Attorney General, the Office of the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may limit or prescribe the White House personnel who may request information concerning such issues from the FBI. (AGG-Dom Part VI.D.2.d)

14.5.2.5 (U) DISSEMINATION OF INFORMATION RELATING TO BACKGROUND INVESTIGATIONS

(U//FOUO) The limitations on dissemination of information by the FBI to the White House under the AGG-Dom do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under E.O. 10450 relating to security requirements for government employment. (AGG-Dom, Part VI.D.2.e)

14.5.3 (U) CONGRESS

(U//FOUO) FBI employees must work through supervisors and the FBI OCA to keep the congressional intelligence committees fully and currently informed of the FBI's intelligence activities as required by the National Security Act of 1947, as amended. Advice on what activities fall within the supra of required congressional notification can be obtained from OCA [A Corporate Policy Directive is forthcoming].

14.6 (U) SPECIAL STATUTORY REQUIREMENTS

(U) Information acquired under the FISA may be subject to minimization procedures and other requirements specified in that Act. (AGG-Dom, Part VI.D.3.a)

(U) Information obtained through the use of National Security Letters (NSLs) under 15 U.S.C. § 1681v (full credit reports) may be disseminated in conformity with the general standards of AGG-Dom, Part VI, and DIOG Section 18.6.6.6.1.8. Information obtained through the use of NSLs under other statutes may be disseminated in conformity with the general standards of the AGG-Dom, Part VI, subject to any specific limitations in the governing statutory provisions (see DIOG Section 18): 12 U.S.C. § 3414(a)(5)(B); 15 U.S.C. § 1681u(f); 18 U.S.C. § 2709(d); 50 U.S.C. § 436(e). (AGG-Dom, Part VI.D.3.b)

(U) Federal Rule of Criminal Procedure 6(e) generally prohibits disclosing "matters occurring before the grand jury." This includes documents, records, testimony of witnesses, or any other evidence deemed relevant by a sitting grand jury. The Attorney General has issued revised Guidelines for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D). On May 15, 2008, the Deputy Attorney General issued a memorandum which provides amplifying guidance as to lawful use and disclosure of 6(e) information. See also AGG-Dom, Part V.A.8 and DIOG Section 18.6.5.3.7.4.5.

14.7 (U) THREAT TO LIFE – DISSEMINATION OF INFORMATION

14.7.1 (U) OVERVIEW

(U//FOUO) The FBI has a responsibility to notify persons of threats to their life or threats that may result in serious bodily injury and to notify other law enforcement agencies of such threats (Extracted from DOJ Office of Investigative Policies, Resolution 20, dated 12/16/96). Depending on the exigency of the situation, an employee, through their supervisor, should notify the appropriate operational division at FBIHQ of the existence of the threat and the plan for notification. That plan may be followed unless advised to the contrary by FBIHQ.

14.7.2 (U//FOUO) INFORMATION RECEIVED THROUGH FISA SURVEILLANCE

(U//FOUO) If information is received through a FISA-authorized investigative technique indicating a threat to life or serious bodily harm within the scope of Section 14.7, the field office case agent responsible for that FISA must immediately coordinate the matter with the FBIHQ SSA responsible for that investigation and an NSLB attorney from the applicable counterintelligence or counterterrorism law unit. These individuals must consult the applicable FISA minimization procedures, consider the operational posture of the investigation, and collectively determine the appropriate manner in which to proceed. FBI executive management may be consulted, as appropriate (e.g., if DIDO or declassification authority is needed). The field office case agent must document the dissemination. If the decision is made not to disseminate the threat information, that decision must be approved by an ASAC or higher and the reasons must be documented in the applicable investigative file.

14.7.3 (U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST INTENDED VICTIMS (PERSONS)

14.7.3.1 (U) WARNING TO THE INTENDED VICTIM (PERSON)

14.7.3.1.1 (U) EXPEDITIOUS WARNINGS TO IDENTIFIABLE INTENDED VICTIMS

(U//FOUO) Except as provided below in Sections 14.7.3.1.1.1 (Exceptions) and 14.7.3.1.2 (Custody or Protectee), when an employee has information that a person who is identified or can be identified through reasonable means (hereafter a "intended victim") is subject to a credible threat to his/her life or of serious bodily injury, the FBI employee must attempt expeditiously to warn the intended victim of the nature and extent of the threat.

14.7.3.1.1.1 (U) EXCEPTIONS TO WARNING

(U//FOUO) An employee is not required to warn an intended victim if:

- A) (U//FOUO) providing the warning to the intended victim is likely to cause equal or greater physical harm to one or more persons;⁸ or
- B) (U//FOUO) the intended victim knows the nature and extent of the specific threat against him/her.

**14.7.3.1.1.2 (U) MEANS, MANNER, AND DOCUMENTATION OF
WARNING/NOTIFICATION OR DECISION NOT TO WARN**

(U//FOUO) The FBI employee, in consultation with his or her supervisor, must determine the means and manner of the warning, using the method most likely to provide direct notice to the intended victim. In some cases, this may require the assistance of a third party. The employee must document on an FD-999 the content of the warning, as well as when, where and by whom it was delivered to the intended victim. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

(U//FOUO) The employee, in consultation with his or her supervisor, may seek the assistance of another law enforcement agency to provide the warning. If this is done, the employee must document on an FD-999 that notice was provided by that law enforcement agency, as well as when, where and by whom (i.e., the name of the other agency's representative) it was delivered. The employee must also document the other agency's agreement to provide a timely warning. The FD-999 must be filed as specified above.

(U//FOUO) Whenever time and circumstances permit, an employee's decision not to provide a warning in these circumstances must be approved by an ASAC or higher. In all cases, the reasons for not providing a warning must be documented by EC or similar successor form in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.1.2 (U) WARNINGS WHEN INTENDED VICTIM IS IN CUSTODY OR IS A PROTECTEE

(U//FOUO) When an employee has information that a person described below is an intended victim, the employee, in consultation with his or her supervisor, must expeditiously notify the law enforcement agency that has protective or custodial jurisdiction of the threatened person.

(U//FOUO) This section applies when the intended victim is:

- A) (U//FOUO) a public official who, because of his/her official position, is provided a protective detail;
- B) (U//FOUO) a participant in the Witness Security Program that is administered by the United States Marshals Service; or
- C) (U//FOUO) detained or incarcerated.

⁸ (U//FOUO) If the equal or greater harm would occur to a Government informant or Agent as a result of his/her participation in an investigation, consideration should be given to extricating that individual from the investigation or taking other appropriate measures in order to minimize the risk.

(U//FOUO) This paragraph does not apply to employees serving on the security detail of the FBI Director or any other FBI protected persons when the threat is to the individual they protect.

**14.7.3.1.2.1 (U) MEANS, MANNER, AND DOCUMENTATION OF
WARNING/NOTIFICATION**

(U//FOUO) The employee, in consultation with his or her supervisor, may determine the means and manner of the notification. When providing notification, the employee shall provide as much information as possible regarding the threat and the credibility of the threat. The employee must document on an FD-999 what he or she informed the other law enforcement agency, and when, where, how (e.g., telephone call, email) and to whom the notice was delivered. The FD-999 must be placed in a zero file or if investigative methods are used, the appropriate investigative file.

**14.7.3.2 (U) NOTIFICATION TO LAW ENFORCEMENT AGENCIES THAT HAVE INVESTIGATIVE
JURISDICTION**

14.7.3.2.1 (U) EXPEDITIOUS NOTIFICATION

14.7.3.2.1.1 (U) THREATS TO INTENDED PERSONS

(U//FOUO) Except as provided in Sections 14.7.3.2.2, when an employee has information that a person (other than a person described above in Section 14.7.3.1.2) who is identified or can be identified through reasonable means is subject to a credible threat to his/her life or of serious bodily injury, the employee must attempt expeditiously to notify other law enforcement agencies that have investigative jurisdiction concerning the threat.

14.7.3.2.1.2 (U) THREATS TO OCCUPIED STRUCTURES OR CONVEYANCES

(U//FOUO) When an employee has information that a structure or conveyance which can be identified through reasonable means is the subject of a credible threat which could cause a loss of life or serious bodily injury to its occupants, the employee, in consultation with his or her supervisor, must provide expeditious notification to other law enforcement agencies that have jurisdiction concerning the threat.

14.7.3.2.2 (U) EXCEPTIONS TO NOTIFICATION

(U//FOUO) An employee need not attempt to notify another law enforcement agency that has investigative jurisdiction concerning a threat:

- A) (U//FOUO) when providing the notification to the other law enforcement agency is likely to cause equal or greater physical harm to one or more persons; or
- B) (U//FOUO) when the other law enforcement agency knows the nature and extent of the specific threat to the intended victim.

(U//FOUO) Whenever time and circumstances permit, an employee's decision not to provide notification to another law enforcement agency in the foregoing circumstances must be

approved by an ASAC or higher. In all cases, the reasons for an employee's decision not to provide notification must be documented in writing in a zero file or if investigative methods are used, the appropriate investigative file.

14.7.3.2.3 MEANS, MANNER, AND DOCUMENTATION OF NOTIFICATION

(U//FOUO) The employee may determine the means and manner of the notification. The employee must document in writing in the applicable investigative file the content of the notification, and when, where, and to whom it was delivered.

14.7.4 (U//FOUO) DISSEMINATION OF INFORMATION CONCERNING THREATS, POSSIBLE VIOLENCE OR DEMONSTRATIONS AGAINST FOREIGN ESTABLISHMENTS OR OFFICIALS IN THE UNITED STATES

(U//FOUO) If information is received indicating a threat to life within the scope of Section 14.7, or possible violence or demonstrations against foreign establishments or officials in the United States, the field office case agent must immediately coordinate the matter with the FBIHQ SSA responsible for the case, who must notify the Department of State (DOS), United States Secret Service (USSS), and any other Government agencies that may have an interest. See Section IV of the 1973 FBI USSS MOU, which is available at http://home.fbinet.fbi/DO/OGC/Memorandums%20of%20Understanding/ss-protective_responsibilities.pdf for the FBI's information sharing responsibilities with the USSS in such cases.

14.7.5 (U) DISSEMINATION OF INFORMATION CONCERNING THREATS AGAINST THE PRESIDENT AND OTHER DESIGNATED OFFICIALS

(U//FOUO) The United States Secret Service (USSS) has statutory authority to protect or to engage in certain activities to protect the President and certain other persons as specified in 18 U.S.C. § 3056. An MOU between the FBI and USSS specifies the FBI information that the USSS wants to receive in connection with its protective responsibilities.

(U//FOUO) Detailed guidelines regarding threats against the President of the United States and other USSS protectees can be found in "Presidential and Presidential Staff Assassination, Kidnapping and Assault." (See the [Violent Crimes PG](#))

15 (U) INTELLIGENCE ANALYSIS AND PLANNING

15.1 (U) OVERVIEW

(U//FOUO) The Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) provide specific guidance and authorization for intelligence analysis and planning. This authority enables the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and planning, the FBI can more effectively discover criminal threats, threats to the national security, and other matters of national intelligence interest, and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. (AGG-Dom, Part IV)

(U//FOUO) In carrying out its intelligence analysis and planning functions, the FBI is authorized to draw on all lawful sources of information, including analysis of historical information in FBI files (open and closed), records and database systems, and information collected from investigative activities permitted without opening an Assessment set forth in DIOG Section 5.1.1.

(U//FOUO) *Note:* In the DIOG, the word “assessment” has two distinct meanings. The AGG-Dom authorizes as an investigative activity an “Assessment,” which requires an authorized purpose as discussed in DIOG [Section 5](#). The United States Intelligence Community (USIC), however, also uses the word “assessment” to describe written intelligence products, as discussed in [Section 15.6.1.2](#) below.

15.2 (U) PURPOSE AND SCOPE

15.2.1 (U) FUNCTIONS AUTHORIZED

(U//FOUO) The AGG-Dom authorizes the FBI to engage in intelligence analysis and planning to facilitate and support investigative activities and other authorized activities. The functions authorized include:

- A) (U//FOUO) Development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, such as domain management as related to the FBI's responsibilities;
- B) (U//FOUO) Research and analysis to produce reports and assessments (analytical products) concerning matters derived from or relevant to investigative activities or other authorized FBI activities; and
- C) (U//FOUO) The operation of intelligence and information systems that facilitate and support investigations and analysis through the compilation and analysis of data and information on an ongoing basis. (AGG-Dom, Introduction B)

15.2.2 (U) INTEGRATION OF INTELLIGENCE ACTIVITIES

(U//FOUO) In order to protect against national security and criminal threats through intelligence-driven operations, the FBI should integrate intelligence activities into all investigative efforts by:

- A) (U//FOUO) Systematically assessing particular geographic areas or sectors to identify potential threats, vulnerabilities, gaps, and collection opportunities in response to FBI collection requirements that support the broad range of FBI responsibilities;
- B) (U//FOUO) Proactively directing resources to collect against potential threats and other matters of interest to the nation and the FBI, and developing new collection capabilities when needed;
- C) (U//FOUO) Continuously validating collection capabilities to ensure information integrity;
- D) (U//FOUO) Deliberately gathering information in response to articulated priority intelligence requirements using all available collection resources, then expeditiously preparing the collected information for analysis and dissemination and promptly disseminating it to appropriate partners at the local, state, national and foreign level; and
- E) (U//FOUO) Purposefully evaluating the implications of collected information on current and emerging threat issues.

15.2.3 (U) ANALYSIS AND PLANNING NOT REQUIRING THE OPENING OF AN ASSESSMENT (SEE DIOG SECTION 5)

(U//FOUO) Without opening an Assessment, an FBI employee may produce written intelligence products that include, but are not limited to, an Intelligence Assessment (analytical product), Intelligence Bulletin and Geospatial Intelligence (mapping) from information already within FBI records. An FBI employee can also analyze information that is obtained pursuant to DIOG Section 5.1.1. If the employee needs information in order to conduct desired analysis and planning that requires the use of Assessment investigative methods beyond those permitted in DIOG Section 5.1.1, the employee must open a Type 4 Assessment in accordance with DIOG Sections 5.6.3.3. The applicable 801H - 807H classification file (or other 801-series classification file as directed in the Intelligence Policy Implementation Guide (IPG)) must be used to document this analysis. See the IPG for file classification guidance.

15.3 (U) CIVIL LIBERTIES AND PRIVACY

(U) The FBI must collect intelligence critical to the FBI's ability to carry out its intelligence and law enforcement mission. While conducting intelligence analysis and planning, the FBI will conduct its activities in compliance with the Constitution, federal laws, the AGG-Dom and other relevant authorities in order to protect civil liberties and privacy.

15.4 (U) LEGAL AUTHORITY

(U) The FBI is an intelligence agency as well as a law enforcement agency. Accordingly, its basic functions extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., (i) 28 U.S.C. §§ 532 note (incorporating P.L. 108-

458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107); and (ii) E.O. 12333 § 1.7(g).

(U//FOUO) The scope of authorized activities under Part II of the AGG-Dom is not limited to “investigations” in a narrow sense, such as solving particular investigations or obtaining evidence for use in particular criminal prosecutions. Rather, the investigative activities authorized under the AGG-Dom may be properly used to provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under AGG-Dom, Part IV, and dissemination of the information to other law enforcement, USIC, and White House agencies under AGG-Dom, Part VI. Accordingly, information obtained at all stages of investigative activity is to be retained and disseminated for these purposes as provided in the AGG-Dom, or in FBI policy consistent with the AGG-Dom, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. (AGG-Dom, Part II)

15.5 (U) INTELLIGENCE ANALYSIS AND PLANNING – REQUIRING A TYPE 4 ASSESSMENT

(U//FOUO) If an FBI employee wishes to engage in intelligence analysis and planning that requires the collection or examination of information not available in existing FBI records or database systems, or from information that cannot be obtained using the activities authorized in DIOG Section 5.1.1, a Type 4 Assessment must be opened and conducted in accordance with DIOG Section 5.6.3.3.

15.6 (U) AUTHORIZED ACTIVITIES IN INTELLIGENCE ANALYSIS AND PLANNING

(U) The FBI may engage in intelligence analysis and planning to facilitate or support investigative activities authorized by the AGG-Dom or other legally authorized activities. Activities the FBI may carry out as part of Intelligence Analysis and Planning include:

15.6.1 (U) STRATEGIC INTELLIGENCE ANALYSIS

(U//FOUO) The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI’s responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security. FBI overviews and analyses may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them. (AGG-Dom, Part IV)

15.6.1.1 (U) DOMAIN MANAGEMENT

(U//FOUO) As part of Strategic Analysis Planning activities, the FBI may collect information in order to improve or facilitate “domain awareness” and may engage in “domain management.” “Domain management” is the systematic process by which the FBI develops cross-programmatic domain awareness and leverages its knowledge to enhance its ability to: (i) proactively identify threats, vulnerabilities, and intelligence gaps; (ii) discover new opportunities for needed intelligence collection and prosecution; and (iii) set tripwires to

provide advance warning of national security and criminal threats. Tripwires are described in DIOG Section 11. Effective domain management enables the FBI to identify significant threats, detect vulnerabilities within its local and national domain, identify new sources and threat indicators, and recognize new trends so that resources can be appropriately allocated at the local level in accordance with national priorities and local threats.

(U//FOUO) The field office “domain” is the territory for which a field office exercises responsibility, also known as the field office’s area-of-responsibility (AOR). Domain awareness is the: (i) strategic understanding of national security and criminal threats and vulnerabilities that exist in the domain; (ii) FBI’s positioning to collect against those threats and vulnerabilities; and (iii) the ability to recognize intelligence gaps related to the domain.

(U//FOUO) Through analysis of previously collected information, supplemented as necessary by properly authorized Type 4 Assessments, domain management should be undertaken at the local and national levels. All National Domain Assessments must be opened and coordinated by the Directorate of Intelligence (DI). Examples of domain management activities include, but are not limited to: collection and mapping of data such as I-94 data, census crime statistics, investigative information, entities in the domain; analysis of trends; source development; and placement of tripwires. See DIOG Section 11 for further discussion of tripwires. Further guidance regarding domain management and examples of intelligence products are contained in the FBIHQ DI policy implementation guide (PG).

(U//FOUO) All information collected during a Type 4 Domain Assessment must be documented in the appropriate Assessment file (801H – 807H classifications), or if obtained without opening an Assessment, in another 800-series classification file as directed in the DI PG. Any time a Type 4 Domain Assessment begins to focus on specific individual(s), group(s), or organization(s), whose activities may constitute a violation of federal criminal law or a threat to the national security, or identifies persons or entities who may be actual or potential targets of or vulnerable to federal criminal activities or national security threats, a separate Assessment (Type 1 & 2 Assessment or a Type 3 Assessment) or Predicated Investigation must be opened to collect information regarding the particular person, or the threat or vulnerability.

(U//FOUO) FBIHQ DI provides specific guidance in its PG regarding, the opening, coordination and purpose for a field office and national domain Type 4 Assessments.

15.6.1.2 (U) WRITTEN INTELLIGENCE PRODUCTS

(U//FOUO) The FBI is authorized to conduct research, analyze information, and prepare reports and intelligence assessments (analytical written products) concerning matters relevant to authorized FBI activities, such as: (i) reports and intelligence assessments (analytical product) concerning types of criminals or criminal activities; (ii) organized crime groups, terrorism, espionage, or other threats to the national security; (iii) foreign intelligence matters; or (iv) the scope and nature of criminal activity in particular geographic areas or sectors of the economy. (AGG-Dom, Part IV)

(U//FOUO) Pursuant to Rule 16 of the Federal Rules of Criminal Procedure, 18 U.S.C. Section 3500, and Department of Justice (DOJ) policy, written intelligence products,

including classified intelligence products, may be subject to discovery in a criminal prosecution, if they relate to an investigation or are produced from information gathered during an investigation. Therefore, a copy of written intelligence products that are directly related to an investigation must be filed in the appropriate investigative file(s) and must include appropriate classification markings.

(U//FOUO) A sub-file named “**INTELPRODS**” exists for all investigative classifications, and a copy of all written intelligence products described above must be placed in the appropriate investigative classification INTELPRODS sub-file.

15.6.1.3 (U) UNITED STATES PERSON (USPER) INFORMATION

(U//FOUO) Reports, Intelligence Assessments, and other FBI intelligence products should not contain USPER information, including the names of United States corporations or business entities, if the pertinent intelligence can be conveyed in an understandable way without including personally identifying information.

(U//FOUO) Intelligence products prepared pursuant to this Section include, but are not limited to: Domain Management, Special Events Management Threat Assessments, Intelligence Assessments, Intelligence Bulletins, Intelligence Information Reports, Weapons of Mass Destruction (WMD) Scientific and Technical Assessments, and Regional Field Office Assessments.

15.6.1.4 (U) INTELLIGENCE SYSTEMS

(U//FOUO) The FBI is authorized to operate intelligence, identification, tracking, and information systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups. (AGG-Dom, Part IV)

(U//FOUO) These systems operate to facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis. Information stored in the systems includes, but is not limited to: investigative files; records obtained from other government agencies through information sharing agreements; open source materials; raw data from FISA and Title III collections; data extracted from source materials such as names, organizations, addresses, and telephone numbers; USIC Foreign Intelligence Collection Requirements, FBI National Collection Requirements and Field Office Collection Requirements; threat reports from law enforcement or the general public; and human source reporting. Access to and use of data contained in these systems is directed by the policies governing the particular system and the laws controlling the data contained therein. Analytic tools such as link charting and geospatial or statistical software are used to analyze the information.

(U//FOUO) When developing a new database, the FBI Office of the General Counsel Privacy and Civil Liberties Unit must be consulted to determine whether a Privacy Impact Assessment (PIA) must be prepared.

15.6.1.5 (U) GEOSPATIAL INTELLIGENCE (GEOINT)

(U//FOUO) Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess and visually depict physical features and geographically-referenced activities on the Earth. As an intelligence discipline, GEOINT in the FBI encompasses all the activities involved in the collection, analysis, and exploitation of spatial information in order to gain knowledge about the national security/criminal environment and the visual depiction of that knowledge. GEOINT also represents a type of information or intelligence product, namely the information and knowledge that is produced as a result of the discipline's activities.

(U//FOUO) Mapping is an activity under GEOINT and may be used in Assessments (Domain Management; Collection Management) and Predicated Investigations.

16 (U) UNDISCLOSED PARTICIPATION (UDP)

16.1 (U) OVERVIEW

(U//FOUO) Undisclosed participation (UDP) takes place when anyone acting on behalf of the FBI, including but not limited to an FBI employee or confidential human source (CHS), becomes a member or participates in the activity of an organization on behalf of the U.S. Government (USG) without disclosing FBI affiliation to an appropriate official of the organization.

16.1.1 (U) AUTHORITIES

(U) The FBI derives its authority to engage in UDP in organizations as part of its investigative and intelligence collection missions from two primary sources.

(U) First, Executive Order (E.O.) 12333 broadly establishes policy for the United States Intelligence Community (USIC). Executive Order 12333 requires the adoption of procedures for undisclosed participation in organizations on behalf of elements of the USIC within the United States. Specifically, the Order provides “. . . [n]o one acting on behalf of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of the any element of the Intelligence Community without first disclosing such person’s intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee.” (E.O. 12333, Section 2.9, Undisclosed Participation in Organizations within the United States). The Order also provides, at Section 2.2, that “[n]othing in [E.O. 12333] shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.”

(U) Second, in addition to its role as member of the USIC, the FBI is also the primary criminal investigative agency of the federal government with authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. This includes the investigation of crimes involving international terrorism and espionage. As a criminal investigative agency, the FBI has the authority to engage in UDP as part of a Predicated Investigation or an Assessment.

(U//FOUO) The FBI’s UDP policy is designed to incorporate the FBI’s responsibilities as both a member of the USIC and as the primary criminal investigative agency of the federal government and, therefore, applies to all investigative and information collection activities of the FBI. It is intended to provide uniformity and clarity so that FBI employees have one set of standards to govern all UDP. As is the case throughout the DIOG, however, somewhat different constraints exist if the purpose of the activity is the collection of positive foreign intelligence that falls outside the FBI’s law enforcement authority. Those constraints are reflected where applicable below.

16.1.2 (U) MITIGATION OF RISK

(U//FOUO) The FBI's policy for UDP uses a risk Assessment model: higher approval levels are required for UDP that carries a greater risk to civil liberties because it is more intrusive. Accordingly, the policy draws a distinction between what is termed "sensitive UDP" and "non-sensitive UDP." These categories focus on the type or purpose of the organization and draw on the concept in the Attorney General Guidelines for Domestic FBI Operations (AGG-Dom) of a "sensitive investigative matter" as the starting point for the distinction.

16.1.3 (U) SENSITIVE UDP DEFINED

(U//FOUO) Sensitive UDP is the undisclosed participation in the activities of a political, religious, or media organization, an academic institution, an organization having an academic nexus, or an organization devoted to advocacy relating to social, religious, or political causes or the education of the public about such causes.

16.1.4 (U) NON-SENSITIVE UDP DEFINED

(U//FOUO) Non-sensitive UDP is undisclosed participation in the activities of any other legitimate organization, such as a business or a club formed for recreational or social purposes. Any doubt about whether an organization falls within the Sensitive UDP category must be resolved by presuming the organization does fall within that category.

16.1.5 (U) TYPE OF ACTIVITY

(U//FOUO) The UDP policy also takes into account the type of activity in which an FBI employee or CHS will engage. For example, in Sensitive UDP, tasking a CHS or FBI employee to join an organization to obtain information about the organization that is not generally known to the public requires a higher approval level than obtaining information provided by an individual who is already a member of the organization. Conduct that may influence the exercise of First Amendment rights by members of the organization or the activities of the organization, the most intrusive UDP, requires legal review and executive approvals. Finally, the UDP policy does not apply to organizations that are not legitimate organizations, as defined below.

16.2 (U) PURPOSE, SCOPE, AND DEFINITIONS**16.2.1 (U) ORGANIZATION**

(U//FOUO) An association of two or more individuals formed for any lawful purpose whose existence is formalized in some manner. The term includes, but is not limited to: social, political, fraternal, professional, business, academic, ethnic-affinity, and religious organizations and includes organizations that meet and communicate primarily on the Internet. For purposes of UDP, an organization does not include a loose group of friends, social contacts, or business associates who may share common interests but whose association lacks any formal structure (e.g., the Rotary is an organization; a group of friends who play poker or meet at a gym for athletics every weekend is not).

16.2.2 (U) LEGITIMATE ORGANIZATION

(U//FOUO) An organization is “legitimate” when it is formed for a lawful purpose and its activities are primarily lawful. (Example: Traditional criminal organizations are not legitimate organizations because their primary purpose is to raise money through the commission of crime. An organization whose primary purpose is to engage in destruction of property as a means to bring public attention to commercial activities that harm the environment is also not a legitimate organization within the meaning of this definition because its primary purpose is to engage in criminal conduct. On the other hand, an organization that seeks to bring attention to a social or political cause by engaging primarily in lawful protest or advocacy, but also some acts of civil disobedience, is a legitimate organization; even though the organization may engage in some unlawful acts, the purpose for which it exists is a lawful one and its activities are primarily lawful.) Any doubt about whether an organization is “legitimate” must be resolved by presuming it is legitimate for purposes of the UDP policy.

16.2.3 (U) PARTICIPATION

(U//FOUO) Taking part in the organization’s activities and interacting with its members within the structure or framework of the organization, whether the individual is tasked to join the organization or is already a member is participation. Occasional social or infrequent ancillary business dealings with members of an organization do not constitute participation. In addition, passive “infrequent attendance”^{*} (five occasions or less) by a person who is not a member of the organization does not constitute “participation.” A CHS or FBI employee who passively attends an organization’s meetings may report any relevant information observed. Regardless of the number of times a CHS or FBI employee attends an organization’s meetings, if he/she becomes involved in the organization’s activities or acts with or on behalf of the organization, the CHS or FBI employee is “participating” for purposes of the UDP policy.

(U//FOUO) **Sensitive UDP** may involve the following:

- A) (U//FOUO) **Academic Institutions**: Participation includes attending classes in person or taking courses on-line. Participation does not include registration: (1) solely for the purpose of obtaining education or training that is relevant to FBI employment or affiliation; or (2) to support credibility in a covert role, provided the FBI employee or confidential human source will not attend classes and will not utilize e-mail or other accounts affiliated with the academic institution to communicate with subjects of an investigation. (See note after paragraph C below)
- B) (U//FOUO) **Media**: Participation includes joining the staff of a publication or a media-centered organization and other activity affecting a publication, such as submitting an article for publication. (See note after paragraph C below)
- C) (U//FOUO) **Political**: Participation includes joining or working on behalf of a political party at any level, a political action group or committee, or a committee formed for the purpose of electing an individual to public office. (See note below)

^{*} (U//FOUO) At time of printing, Section 16.2.3 rule for passive “infrequent attendance” was pending final review and approval by the Attorney General. Please always check the online DIOG available on the FBI Intranet for the current and official DIOG.

(U//FOUO) **Note: “infrequent attendance”** (see footnote #8 above) at an event or activity of a sensitive organization as defined in DIOG Section 16.1.3 by a tasked CHS requires approval as set forth in the **“Special Rule for Other Sensitive Organizations.”** See DIOG Sections 18.5.1.3.1 and 18.5.5.3.D.

- D) (U//FOUO) **Religious:** Participation includes joining the religious organization or participating in activities of the organization that are central to the function of the organization, whether or not open to the public. Attendance at a social event sponsored by the religious organization that is open to the public will generally not constitute “participation.”

(U//FOUO) **Note: “infrequent attendance”** (see footnote #8 above) at a religious service by an employee or a tasked CHS requires approval as set forth in the **“Special Rule for Religious Services.”** See DIOG Sections 18.5.1.3.1 and 18.5.5.3.C.

(U//FOUO) Examples of Participation:

- A) (U//FOUO) **Example 1:** An FBI CHS is tasked to begin attending religious services at a particular religious facility on a regular basis. Is this participation?

(U//FOUO) **Response to Example 1:** This would constitute “participation” because religious services are central to the function of the religious organization and, from the outset, the FBI intends for the CHS to become a regular participant.

- B) (U//FOUO) **Example 2:** In a Predicated Investigations, an FBI CHS is tasked to attend, as a passive observer, the organizational meeting of “No Tree Unserved,” an environmental group that is being advertised as “more effective than ELF in saving the planet” and to report back on any relevant information learned. Is this participation?

(U//FOUO) **Response to Example 2:** This is not “participation” because it is one-time or “infrequent attendance” (five occasions or less) by a person who is not a member of the group. If this tasking took place during an Assessment, SSA approval would be required before tasking a CHS to passively attend activities of a sensitive organization, as defined in DIOG Section 16.3.1.

- C) (U//FOUO) **Example 3:** The CHS from Example 2 reports that the group has a mailing list and a twitter feed. The FBI tasks the CHS to sign up for both. Is the CHS now “participating” in No Tree Unserved?

- D) (U//FOUO) **Response to Example 3:** By virtue of joining the mailing list or the twitter feed, the CHS is participating in the group.

16.2.3.1 (U) UNDISCLOSED PARTICIPATION

(U//FOUO) Participation is “undisclosed” when anyone acting on behalf of the FBI, including but not limited to an FBI employee or CHS, participates in the activity of the organization on behalf of the USG without disclosing FBI affiliation to an appropriate official of the organization. A CHS who participates in an organization entirely on his own behalf and who is not tasked by the FBI to obtain information or engage in other activities in that organization is not engaging in UDP—regardless whether the CHS volunteers information to the FBI and regardless whether the CHS’s affiliation with the FBI is known. If the CHS is tasked to obtain specific information or to take specific action, his/her subsequent participation to fulfill that task is on behalf of the FBI.

16.2.3.2 (U//FOUO) INFLUENCING THE ACTIVITIES OF THE ORGANIZATION

(U//FOUO) UDP influences the activities of the organization when it has a significant effect on the organization's agenda, course of business, core activities, or future direction. Simply voting or expressing an opinion on these matters as a member will generally not fall within this definition.

16.2.3.3 (U//FOUO) INFLUENCING THE EXERCISE OF FIRST AMENDMENT RIGHTS

(U//FOUO) UDP influences the exercise of First Amendment rights of the members of an organization when it substantially affects the agenda of an organization with respect to the advocacy of social, religious, or political causes, the education of the public about such causes, or the practice of religion.

16.2.3.4 (U) APPROPRIATE OFFICIAL

(U//FOUO) An individual with actual or apparent authority to act on behalf of the organization in directing or authorizing its activities or monitoring its membership. If the CHS or FBI employee whose participation is at issue is an official of the organization, his or her knowledge alone is not sufficient to remove the participation from being UDP. Disclosure must be made to an additional official with actual or apparent authority to act on behalf of the organization in order for the activity of the CHS or FBI employee not to be UDP.

16.2.3.5 (U) SENSITIVE UNDISCLOSED PARTICIPATION

(U//FOUO) Undisclosed participation in the activity of:

- A) (U//FOUO) A political, religious, or media organization, an academic institution, or an organization having an academic nexus; or
- B) (U//FOUO) An organization that has as a significant purpose the advocacy of social, religious, or political causes or the education of the public about such causes; or
- C) (U//FOUO) Any other organization, in which UDP should, in the judgment of the FBI employee proposing the UDP or the approving official, be brought to the attention of senior FBI officials.

(U//FOUO) Refer to the definitions in DIOG Section 10.2 relating to Sensitive Investigative Matter (SIM) for the definitions of political organization, religious organization, and academic nexus. The definition of "media organization" is broader than news media and includes any organization that has as a significant purpose the publication or broadcast of news or any other information.

(U//FOUO) Any doubt about whether an organization has as a significant purpose the advocacy of social, religious, or political causes, the education of the public about such causes, or the practice of religion, must be resolved by presuming the organization has such a purpose.

16.2.3.6 (U) ALREADY A MEMBER OF THE ORGANIZATION OR A PARTICIPANT IN ITS ACTIVITIES

(U//FOUO) This means that the individual who is acting on behalf of the FBI has not at any time been directed by the FBI, by a law enforcement agency or by a member USIC to join the organization or participate in its activities.

16.3 (U) REQUIREMENTS FOR APPROVAL**16.3.1 (U) GENERAL REQUIREMENTS**

(U//FOUO) UDP is permitted in either an Assessment or a Predicated Investigation subject to the approval requirements and limitations set forth below. The requirement for UDP authorization applies only when the information furnished by the CHS or FBI employee derives from being a member or participating in the activities of organization by the CHS or FBI employee. UDP of an FBI employee will always be considered as a tasked activity and subject to applicable supervisory approvals. Approval granted for UDP in an Assessment or investigation will generally apply for the duration of the Assessment or investigation unless there is a change of circumstances that implicate either another approval requirement in this subsection or the approval standards listed in subsection 16.5. The approval requirements set forth below are in addition to the required supervisory approvals for undercover operations (UCO) established by the Attorney General Guidelines for FBI Undercover Operations (AGG-UCO) and the required supervisory approvals to open and use a CHS established by the Attorney General Guidelines on the Use of FBI Confidential Human Sources (AGG-CHS) and the FBI's Confidential Human Source Policy Implementation Guide (CHSPG).

16.3.1.1 (U) UNDERCOVER ACTIVITY

(U//FOUO) UDP as an undercover activity by an FBI Undercover Employee (UCE) is subject to the policy and procedures for undercover operations contained within the AGG-UCO, the AGG-Dom, and FBI policy, and may only occur in a Predicated Investigation. UDP as an undercover activity by a UCE is not permitted in an Assessment.

16.3.1.2 (U) CONCURRENT APPROVAL

(U//FOUO) The approval to open a CHS and approval for UDP may be given concurrently if UDP is a reason the CHS is being opened in the first instance (e.g., a CHS is recruited and opened because he is a member of an anti-government militia group). If a CHS who is already opened will engage in UDP under circumstances that are significantly different than those originally approved (e.g., a CHS in a narcotics investigation is tasked to join a white supremacist group), new UDP approval is required. Other review and approval requirements as specified below may also apply. If a CHS already approved for UDP in one organization is tasked to participate in another organization on behalf of the FBI, new UDP approval is required.

16.3.1.3 (U) DELEGATION AND "ACTING" STATUS

(U//FOUO) The approval authorities described in Sections 16.3.1.4 and 16.3.1.5 may **not** be delegated. An FBI employee properly designated to serve in an "acting" capacity may take action to approve or disapprove as if regularly appointed to the position.

(U//FOUO) Sections 16.3.1.4 and 16.3.1.5 below, which set forth the AG approved UDP policy, reference time periods for approvals. By FBI policy, some of these time periods have been shortened. The schedule established in Section 16.9, which sets forth the FBIHQ Approval Process for UDP Requests, is designed to ensure all FBIHQ approvals are obtained within the AGG-Dom required time periods.

16.3.1.4 (U) SPECIFIC REQUIREMENTS FOR GENERAL UNDISCLOSED PARTICIPATION (NON-SENSITIVE UDP)

16.3.1.4.1 (U//FOUO) OBTAINING INFORMATION AS A MEMBER OR PARTICIPANT IN THE ACTIVITIES OF AN ORGANIZATION

- A) (U//FOUO) In Assessments, approval by a supervisory special agent (SSA) is required if: (i) a CHS who is already a member or participant in an organization is tasked to obtain information on behalf of the FBI, or (ii) a CHS will be tasked to join the organization or participate in its activities to obtain information. As noted above, approval for this UDP may be granted concurrently when approval to open the source is granted.
- B) (U//FOUO) In a Predicated Investigation, no supervisory approval is required if: (i) a CHS who is already a member or participant in an organization is tasked to obtain information on behalf of the FBI, or (ii) a CHS will be tasked to join the organization or participate in its activities to obtain information. SSA approval is required to task an FBI employee to join the organization or participate in its activities to obtain information. If the UDP is part of an undercover operation (UCO), approval requirements for that operation apply, including review by the CDC and approval of the SAC.

16.3.1.4.2 (U//FOUO) ENGAGING IN CONDUCT FOR THE PURPOSE OF INFLUENCING THE ACTIVITIES OF THE ORGANIZATION OR CONDUCT THAT MAY INFLUENCE THE EXERCISE OF FIRST AMENDMENT RIGHTS BY MEMBERS OF THE ORGANIZATION

(U//FOUO) Regardless of prior membership or participation:

- A) (U//FOUO) In an Assessment, a CHS participating in an organization in an undisclosed capacity is not permitted to engage in conduct on behalf of the FBI for the purpose of influencing the activities of the organization or that may influence the exercise of First Amendment rights by members of the organization.
- B) (U//FOUO) In a Predicated Investigation, if a CHS or FBI employee is to engage in conduct on behalf of the FBI for the purpose of influencing the activities of an organization, review by the CDC and approval by the SAC are required.
- C) (U//FOUO) In a Predicated Investigation, if a CHS or FBI employee is to engage in conduct that may influence the exercise of First Amendment rights by members of the organization, prior review by the Office of General Counsel (OGC) is required. If OGC determines that the UDP is not likely to influence the exercise of First Amendment rights by members of the

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

organization, the Assistant Director (AD) of the FBI Headquarters operational division exercising oversight for the investigation may approve the UDP. If the UDP is part of an UCO, approval requirements for that operation apply. If approved, notification must be made by the requesting field office to the Sensitive Operations Review Committee (SORC) within 10 days of approval.

- D) (U//FOUO) In a Predicated Investigation, if a CHS or FBI employee is to engage in conduct that is intended to influence the exercise of First Amendment rights by members of the organization, or if there has been a determination by OGC that the UDP is likely to influence the exercise of First Amendment rights by members of the organization, prior approval by the Director, the Deputy Director, or an Executive Assistant Director is required. Such requests will be considered following review by OGC and other review required by FBI policy, such as that conducted by the Undercover Operations Review Committee. In determining whether to approve such activity, the approving official will consider whether such UDP is necessary to meet a significant investigative goal that cannot be achieved without this level of participation. If approved, notification must be made by the requesting field office to the SORC within 10 days of approval.

16.3.1.5 (U) SPECIFIC REQUIREMENTS FOR SENSITIVE UNDISCLOSED PARTICIPATION (SENSITIVE UDP)

16.3.1.5.1 (U//FOUO) OBTAINING INFORMATION AS A MEMBER OR A PARTICIPANT IN THE ACTIVITIES OF A SENSITIVE ORGANIZATION

- A) (U//FOUO) Subject to subsection 16.3.1.5.2 below, in Assessments and Predicated Investigations, if the CHS is already a member of the organization or a participant in its activities and is tasked to obtain information, SSA approval is required. As noted above, when a CHS is opened to conduct these activities, SSA approval for UDP may be granted concurrently when the source is opened.
- B) (U//FOUO) In Assessments and Predicated Investigations, if a CHS or FBI employee is tasked to join an organization or participate in its activities and obtain information, review by the CDC and prior approval of the SAC is required. If approved, the field office must notify the SORC within 10 days following this approval. If the UDP is part of an UCO, approval requirements for that operation apply.

16.3.1.5.2 (U//FOUO) OBTAINING "INSIDER" INFORMATION DURING AN ASSESSMENT

(U//FOUO) If a CHS, who is already a member of or participant in a sensitive organization, is tasked to obtain information that is not generally known to regular members or participants, CDC review and prior SAC approval are required. If the CHS is tasked to join the organization for the purpose of obtaining this type of information, review by OGC and approval by the operational division's AD with program oversight responsibility are required. If UDP is approved, the field office must notify the SORC within 10 days.

16.3.1.5.3 (U//FOUO) ENGAGING IN CONDUCT THAT MAY INFLUENCE THE ACTIVITIES OF THE ORGANIZATION OR THE EXERCISE OF FIRST AMENDMENT RIGHTS BY MEMBERS OF THE ORGANIZATION

(U//FOUO) Regardless of prior membership or participation status:

- A) (U//FOUO) In an Assessment, a CHS participating in an organization in an undisclosed capacity is not permitted to engage in conduct on behalf of the FBI for the purpose of influencing the activities of the organization or conduct that may influence the exercise of First Amendment rights by members of the organization.
- B) (U//FOUO) In a Predicated Investigation, if a CHS or FBI employee is to engage in conduct on behalf of the FBI for the purpose of influencing the activities of an organization or conduct that may influence the exercise of First Amendment rights by members of the organization, prior review by OGC is required. If OGC determines that the UDP is not likely to influence the exercise of First Amendment rights by members of the organization, the AD of the FBI Headquarters operational division exercising oversight for the investigation may approve the UDP. If approved, the requesting field office must notify the SORC within 10 days of approval.
- C) (U//FOUO) In a Predicated Investigation, if a CHS or FBI employee is to engage in conduct on behalf of the FBI that is intended to influence the exercise of First Amendment rights by members of the organization, or if there has been a determination by OGC that the UDP is likely to influence the exercise of First amendment rights by members of the organization, prior approval by the Director is required. The Director will only consider such requests following review by OGC and the SORC or other similar review, including that conducted by the Undercover Operations Review Committee. In determining whether to approve such activity, the Director will consider whether such UDP is necessary to meet a significant investigative goal that cannot be achieved without this level of participation.

16.4 (U) SUPERVISORY APPROVAL NOT REQUIRED

(U//FOUO) Participation in the activities of an organization under the following circumstances does not require supervisory approval:

- A) (U//FOUO) A CHS, who is already a member of an organization or who joins on his or her own behalf, volunteers information not in response to a specific request or tasking by the FBI.
- B) (U//FOUO) The information to be obtained will derive solely from attending events or activities that are open to the general public on the same terms and conditions as members of the general public. **Note: If the public event is a religious service, see the “Special Rule for Religious Services” in DIOG Section 18.5.1.3.1.1. If the attendance is at an event or activity of a sensitive organization, see the “Special Rule of Other Sensitive Organizations” in DIOG Section 18.5.1.3.1.2.**
- C) (U//FOUO) The organization is an entity that is openly acknowledged by a foreign government to be directed or operated by that foreign government.
- D) (U//FOUO) The organization is reasonably believed to be acting on behalf of a foreign power and its U.S.-based membership is reasonably believed to consist primarily of individuals who are not United States persons (USPERs).
- E) (U//FOUO) The organization is not considered a legitimate organization because it was not formed for a lawful purpose or because its primary purpose is to engage in unlawful activity. (*Note: Some organizations may have a lawful purpose but also contain one or more smaller factions that are dedicated to committing criminal acts or otherwise violating the laws of the United States. Authorization is not required if the participation is entirely limited to the activity of the smaller faction. Any doubt about whether the UDP can or will be so limited should be resolved by assuming it cannot be so limited.*)

16.5 (U) STANDARDS FOR REVIEW AND APPROVAL

(U//FOUO) An FBI employee proposing UDP or an approving official reviewing a request for UDP must consider the following factors:

- A) (U//FOUO) The potential benefits to national security or the public welfare to be achieved by obtaining information through the undisclosed participation in the organization;
- B) (U//FOUO) Whether the proposed course of action is a reasonable means to achieve those benefits and is appropriate under the circumstances;
- C) (U//FOUO) Whether the course of action is the least intrusive investigative method feasible under the circumstances;
- D) (U//FOUO) Whether the anticipated benefits outweigh any adverse impact on civil liberties, privacy, or other rights that may be affected; and
- E) (U//FOUO) Whether there is a foreseeable risk of more than a *de minimis* adverse impact on civil liberties, privacy, or other rights and, if so, whether appropriate safeguards including limits on duration and scope, have been considered and will be imposed to ensure adherence with applicable law and to minimize such risk.

(U//FOUO) For UDP undertaken to collect foreign intelligence that does not concern criminal activities or threats to the national security (“positive foreign intelligence”), an approving official must determine, in addition to the factors listed above, that such participation:

- A) (U//FOUO) Is consistent with the admonition in the AGG-Dom to operate openly and consensually with USPERs to the extent practicable; and
- B) (U//FOUO) Is essential to achieving lawful purposes.

(U//FOUO) In addition to the considerations specified above, use of a CHS is subject to the policy and procedures specified in the AGG-CHS and the FBI’s CHSPG. If there is any inconsistency between the CHSPG and this policy, this policy controls.

(U//FOUO) Participation by an FBI employee in an undercover capacity is subject to the policy and procedures for undercover operations contained within the Attorney General Guidelines for FBI Undercover Activities (AGG-UCO), the AGG-Dom and FBI policy. (See DIOG Section 18, the Undercover and Sensitive Operations PG, and the National Security Undercover Operations (NSUCO) PG.

(U//FOUO) Questions concerning UDP should be discussed with the CDC and OGC. Questions about whether or not an organization is considered a “legitimate” organization must be referred to OGC.

16.6 (U) REQUESTS FOR APPROVAL OF UNDISCLOSED PARTICIPATION

(U//FOUO) SSA approval for UDP must be documented in an appropriate file¹⁰. The documentation must indicate that the SSA considered the factors set forth in subsections 16.5 in approving the proposed UDP. The documentation must also identify or describe the organization,

¹⁰ (U//FOUO) If the UDP is for a CHS, the approval must be documented in the CHS’s DELTA file. The approval document must reference the investigative file in which UDP will be conducted.

describe the anticipated participation by the CHS or FBI employee in the organization and the expected duration of that participation, contain an explanation why UDP is the least intrusive alternative feasible under the circumstances, and, if the purpose of the investigation or Assessment is the collection of foreign intelligence from USPERs who are members of the organization, contain an explanation of why dealing openly and consensually with those persons is not feasible.

(U//FOUO) A UDP request must contain the following information:

- A) (U//FOUO) The name of the organization and a description of its mission and activity.
- B) (U//FOUO) A description of the investigative or Assessment plan with specific details regarding the anticipated participation by the CHS or FBI employee in the organization; an explanation of how such participation will further the Assessment or Predicated Investigation or assist in the collection of foreign intelligence; and a statement regarding the expected duration of the UDP.
- C) (U//FOUO) An explanation why UDP is the least intrusive alternative feasible under the circumstances, and additionally, if the purpose of the investigation or Assessment is the collection of foreign intelligence from USPERs who are members of the organization, an explanation why dealing openly and consensually with those persons is not feasible.
- D) (U//FOUO) An explanation whether the participation in the organization by the CHS or FBI employee is intended to influence the activities of the organization or may influence the exercise of First Amendment rights by members of the organization, and, if it may, how it might influence these activities.
- E) (U//FOUO) A description of any safeguards that will be implemented to minimize the impact on the exercise of First Amendment rights, if applicable.
- F) (U//FOUO) If expedited review is requested, a description of the operational reasons for that request and a statement of the date by which the request must be approved or denied.

(U//FOUO) Review of UDP requests should be accomplished in an expeditious manner. In all events, review and approval by FBI Headquarters elements should be accomplished within 30 days of the submission of the request. If an earlier approval is needed for operational reasons, the basis for expedited review must be clearly stated in the request. Approval by an FBI Headquarters element will be noted in correspondence returned to the requesting field office that is to be retained in the appropriate investigative file.

16.7 (U) DURATION

(U//FOUO) The duration of UDP is limited by the Predicated Investigation or Assessment in which it is authorized and must be terminated at the conclusion of the investigation or the Assessment unless: (i) the Assessment results in the opening of a Predicated Investigation as to which the UDP will contribute, or (ii) circumstances warrant the temporary continuation of the UDP by the CHS in the organization because a new Assessment or Predicated Investigation is planned that will utilize the CHS's placement and such temporarily-continued UDP activity is reviewed by the CDC and approved by an ASAC. Future tasking to join or participate in the activities of an organization in which a CHS or undercover employee (UCE) was previously a member requires new approval.

16.8 (U//FOUO) SENSITIVE OPERATIONS REVIEW COMMITTEE (SORC)**16.8.1 (U//FOUO) SORC NOTIFICATION**

(U//FOUO) As indicated above, the field office will provide notification to the SORC, through the AD of the FBI Headquarters division with oversight responsibility for the investigation or Assessment concerning the following approved UDP:

- A) (U//FOUO) If in the course of an Assessment involving sensitive UDP, a CHS is tasked to join an organization or participate in its activities, or
- B) (U//FOUO) In the course of a Predicated Investigation involving either sensitive or non-sensitive UDP, a CHS or FBI employee is tasked to undertake a role that may tend to influence the exercise of First Amendment rights by members of the organization but that OGC has determined is not likely to influence the exercise of such rights.

(U//FOUO) Such notifications will be received by the FBI staff supporting the SORC. The SORC will receive reports of such UDP from the supporting staff on a schedule and in a form to be determined by the SORC.

16.8.2 (U//FOUO) SORC REVIEW

(U//FOUO) The SORC will review any proposed sensitive UDP in an organization that is purposely taken to influence the exercise of First Amendment rights by members of the organization or that has been determined by OGC to likely influence the organization's activity. The request will be reviewed by the OGC which will provide advice to the SORC on the matter. The SORC will prepare a written recommendation regarding the request and forward the request and its recommendation to the Director for approval. The decision of the Director will be documented and forwarded to the appropriate field office.

(U//FOUO) For more details regarding the organization and functions of the SORC, see DIOG Section 10.2 above and Section 16.9 below.

16.9 (U) FBIHQ APPROVAL PROCESS OF UDP REQUESTS**16.9.1 (U) SUBMITTING THE UDP REQUEST TO FBIHQ**

(U//FOUO) After appropriate coordination and approval within the field office, a UDP request to FBIHQ must be submitted with an EC addressed to the appropriate FBIHQ operational unit with responsibility for oversight of the investigation. The EC must contain the information required by subsection 16.6 and request approval of the UDP. If the proposed UDP will require review by the SORC, the EC should also address the factors the SORC will consider in making its recommendation to the Director (see DIOG Section 10.2.3). If expedited review is required, the circumstances requiring expedition must be clearly delineated in the EC, including the date by which the field office or FBIHQ division requires the determination. Review and approval authorities will take note of these special circumstances and complete their actions as expeditiously as possible. The time frames set forth below in sections 16.9.2 and 16.9.3 will apply to routine UDP requests. Absent unusual circumstances, the FBIHQ approval processes

discussed below should be completed within 30 calendar days from the receipt of the initial submission by the field office or FBIHQ division.

(U//FOUO) *Note:* A CHS with prior UDP authority may require new UDP authority if his/her role within a particular organization changes. For example, in a Predicated Investigation with SAC approval a CHS may be tasked to join an organization and participate in its activities. If the CHS subsequently moves into a position where the level of participation may be seen as influencing the activities of the organization, then new UDP approval would be required. While the new UDP approval request is pending at FBIHQ, the field office may continue to accept intelligence from the CHS but may not actively task the CHS to participate in any activities beyond those already approved under the prior UDP.

16.9.2 (U//FOUO) ASSESSMENTS – CHSS TASKED TO JOIN SENSITIVE ORGANIZATIONS AND OBTAIN INSIDER INFORMATION

(U//FOUO) In Assessments, if the UDP is considered sensitive and involves tasking a CHS to join an organization for the purpose of obtaining insider information, the FBIHQ operational unit with responsibility for oversight of the Assessment will prepare a response EC for review by OGC (Investigative Law Unit (ILU) in criminal, DT, WMDD, and CyD investigations and National Security Law Branch (NSLB) in national security investigations) and approval by the AD of the operational Division. The reviewing OGC unit and the operational division AD will apply the standards in Section 16.5 above in reviewing and deciding whether to approve. This action should be completed within 10 business days of receipt of the request from the field office. Notice to the SORC will be included in the response EC and satisfies the requirement for notice by the field office.

16.9.3 (U//FOUO) PREDICATED INVESTIGATIONS – UDP REQUESTS INTENDED TO OR WHICH MAY INFLUENCE THE ACTIVITIES OF AN ORGANIZATION OR THE EXERCISE OF FIRST AMENDMENT RIGHTS BY ITS MEMBERS

(U//FOUO) When the field office determines that UDP during a Predicated Investigation is intended to or may influence the activities of an organization or the exercise of First Amendment rights of the organization's members:

- A) (U//FOUO) Within three (3) business days of the receipt of the EC, the responsible FBIHQ operational unit must submit the field office's EC to OGC (Attention ILU in criminal, DT, WMDD and CyD investigations or Attention NSLB, in national security investigations) for a determination: (1) whether the UDP is intended or likely to influence the activities of the organization or the exercise of First Amendment rights of the members of the organization; (2) if the UDP is intended or likely to influence the activities of the organization, whether or not it is intended or likely to influence the exercise of First Amendment rights of the members of the organization.
- B) (U//FOUO) Within five (5) business days of the receipt of the EC from the FBIHQ operational unit, OGC must review the request and submit its written determination as follows:
 - 1) (U//FOUO) If OGC determines the UDP is not likely to influence the activities of the organization or the exercise of First Amendment rights of the members of the organization, the request, together with OGC's written determination, must be returned to the

responsible FBIHQ operational unit. The responsible FBIHQ operational unit must advise the requesting field office and the SORC of OGC's determination by EC within five (5) business days of receipt. Upon receiving this advice, the requesting field office must then obtain the appropriate UDP approval at the field office level pursuant to subsections 16.3.1.4, 16.3.1.5, and 16.5.

- 2) (U//FOUO) If OGC determines the UDP is likely to influence the activities of the organization but is not likely to influence the exercise of First Amendment rights of the members of the organization, OGC must provide a written determination to the responsible FBIHQ operational unit. The responsible FBIHQ operational unit must include OGC's determination in a recommendation EC to the responsible AD within five (5) business days. The responsible AD must determine within ten (10) business days whether to grant or deny the UDP applying the standards established in Section 16.5 above. Whether the responsible AD approves or denies the UDP, the responsible FBIHQ operational unit must notify by EC the field office and the SORC within three (3) business days of the AD's decision.
- 3) (U//FOUO) If OGC determines the UDP is likely to influence the exercise of First Amendment rights of the members of the organization:
 - a) (U//FOUO) For non-sensitive UDP, OGC must provide a written determination to the responsible FBIHQ operational unit. Within five (5) business days, the responsible FBIHQ operational unit must include OGC's determination in a recommendation EC to the Director, Deputy Director, or Executive Director, as appropriate. The approving official must determine within ten (10) business days whether to grant or deny the UDP applying the standards established in Section 16.5 above. Whether the approving official approves or denies the UDP, the responsible FBIHQ operational unit must notify the SORC and requesting field office within three (3) business days of the decision.
 - b) (U//FOUO) For sensitive UDP, OGC must provide a written determination to the responsible FBIHQ operational unit and to the SORC. Within five (5) business days, the responsible FBIHQ operational unit must submit an EC setting forth its recommendation to the SORC for consideration. The SORC must review the request along with OGC's determination and provide a recommendation regarding approval or disapproval to the Director within thirty (30) calendar days of the initial submission from the field office absent unusual circumstances. The SORC staff must include the SORC's recommendation in a recommendation EC to the Director. The Director will determine whether to grant or deny the UDP applying the standards established in Section 16.5 above. The responsible FBIHQ operational unit must notify the requesting field office and the SORC by EC of the Director's decision.

16.9.4 (U//FOUO) PROCEDURES FOR APPROVING EMERGENCY UDP REQUESTS THAT OTHERWISE REQUIRE FBIHQ APPROVAL

(U//FOUO) FBI policy permits departures from DIOG requirements in special circumstances (see DIOG Section 2.7). If UDP that would otherwise require FBIHQ approval (e.g., an activity intended to influence the activity of an organization, or influence members of an organization First Amendment rights) is urgently needed because of the immediacy or gravity of a threat to the safety of persons or property, threats to the national security, or loss of a significant investigative opportunity, the SAC, with concurrence from the Deputy Assistant Director (DAD) of the FBIHQ operational section with oversight responsibilities for the investigation and a

Deputy General Counsel of OGC, may authorize the UDP. As soon as practicable after granting emergency UDP authority, but within 48 hours, the SAC or the FBIHQ DAD must provide an EC to the SORC, the operational division AD, and the GC describing the circumstances and necessity for authorizing emergency UDP, as well as whether continuing UDP authority is being requested.

(U//FOUO) Upon receipt of the EC, the SORC staff shall obtain a determination from the relevant OGC Deputy General Counsel whether AD or Director approval is required and handle the matter accordingly. The operational division AD may disapprove the continuation of the UDP. If the UDP activity is continued and the level of UDP would have required SORC consideration and Director approval if proposed in the normal course, the SORC staff will notify other members of the SORC and describe the UDP. Unless a SORC member objects to the UDP upon receiving notice from the SORC staff, the UDP may continue until it is reviewed at the next scheduled SORC meeting when the SORC will make a formal recommendation to the Director whether the activity should continue. If a SORC member objects to the level of UDP activity, an ad hoc meeting must be called.

(U//FOUO) Notwithstanding the above, all UDP must be carried out in a manner consistent with the Constitution and the laws of the United States.

16.10 (U) UDP EXAMPLES

A) (U//FOUO) **Example A:** Andrew is a bartender in a local bar. He hears customers talking about a plan to bring merchandise stolen from a freight container into the store next door and offer it for sale. Andrew contacts the FBI and tells the duty agent about the conversation. The agent taking the complaint asks Andrew if he would be interested in continuing to provide updates on this plan as he hears about it. Ultimately, the bartender is opened as a CHS.

(U//FOUO) **Analysis A:** This is not UDP in an organization. Andrew is participating in the conversations at the bar (not “participating” in an “organization’s” activities). No UDP authorization is required.

B) (U//FOUO) **Example B:** Bart works on the loading dock of a regional distribution center. Truck deliveries from manufacturers are made to the distribution center; the merchandise is off loaded and organized for shipment throughout the country in company trucks. Bart observes that delivery trucks frequently deliver counterfeit products with the full knowledge of the manager. These products are then merged with other products for shipment to retail stores. Bart mentions this to an FBI agent and agrees to provide the FBI information on a regular basis about the operation. Bart is opened as a CHS and is told to record the license plates of trucks delivering counterfeit merchandise, the names of drivers, and the names of employees who assist in the ring.

(U//FOUO) **Analysis B:** This is UDP in an organization: Bart was initially acting on his own behalf in participating in the activities of the organization, but he is now participating on behalf of the FBI because he has been tasked to obtain specific information. In an Assessment, SSA approval is required for this non-sensitive UDP which may be given at the same time the individual is opened as a CHS. In a Predicated Investigation, no additional approval is required to utilize the CHS in this manner. Please note: there is adequate predication in the example discussed above to open a Predicated Investigation.

C) (U//FOUO) **Example C:** Cindy regularly spends Saturday with a local group known as “friends of the environment” that undertakes cleanup projects, such as removing rubbish from waterfront areas and wilderness trail parks. Cindy hears members of the group discussing a large commercial development that is under construction taking up what had been a picturesque spot on the river. Like other members of the group Cindy is outraged at developers who promoted the development and with city officials who approved it. She hears some members of the group discussing Citizen’s Alliance, another organization to which they belong. Citizen’s Alliance, in addition to holding peaceful demonstrations about the lack of environmental concern the project is showing, plans to take a more activist role in preventing the construction from moving forward. Cindy is uncomfortable with that idea, and she contacts the FBI about Citizen’s Alliance. The FBI has limited source reporting that Citizen’s Alliance is responsible for damage to cell phone towers built along a wilderness trail. The FBI asks Cindy to join Citizen’s Alliance and to report to the FBI on its activities. Cindy agrees and the FBI office wants to open Cindy as a CHS.

(U//FOUO) **Analysis C:** UDP approval is required. Because Citizen’s Alliance advocates through demonstrations and public education about environmental issues, it is a legitimate group even though it may also be using destruction of property as a tool to deliver its message. The Citizen’s Alliance purpose and activities make the participation by the CHS “sensitive UDP.” These facts, i.e., source reporting that the group is responsible for the cell phone towers and Cindy’s reporting that the group is planning a more activist role with respect to the new development, would support opening an Assessment on the group. Sensitive UDP during an Assessment requires CDC review and SAC approval to task a CHS to join and report on general information about the group. Concurrent approval can be requested in an EC to open Cindy as a CHS and approve her UDP in this sensitive organization. The SORC must be notified within 10 business days of the UDP approval.

D) (U//FOUO) **Example D:** Later, a Predicated Investigation is opened on the Citizen’s Alliance based on confirmation of the reports about damage to the cell phone towers. Cindy, who is now a member of Citizen’s Alliance, is asked to provide information about the group, such as its membership and how it raises money. Cindy tells her handling agent that information is very tightly held within the organization.

(U//FOUO) **Analysis D:** CDC review, SAC approval, and notice to the SORC are required for this new tasking. Although now a member of the group, Cindy first joined Citizen’s Alliance at the direction of the FBI; accordingly, her status will always be as someone tasked to join and provide information.

E) (U//FOUO) **Example E:** Cindy is asked to be the secretary of the Citizen’s Alliance (a sensitive organization). This position involves performing administrative tasks and taking notes at the group’s meetings. As a CHS, Cindy wants to continue to provide information to the FBI about the group’s possible criminal activities.

(U//FOUO) **Analysis E:** The field office submits the request to FBIHQ to obtain a determination whether Cindy’s UDP may influence the activities of the organization or the exercise of First Amendment rights by its members. Absent other facts indicating that Cindy’s position is something more than merely administrative, OGC would conclude that Cindy’s position would not likely influence the activities of the organization nor the exercise of First Amendment rights by its members. The request, together with OGC’s written determination, will be returned to the responsible FBIHQ operational unit, which will advise the requesting field office and the SORC of OGC’s determination. The field office will then be responsible for approving or denying the UDP request pursuant to subsections 16.3.1.5, and 16.5.

- F) (U//FOUO) **Example F:** Cindy has now become a key member of Citizen's Alliance (a sensitive organization) and she has been elected to the position of "activities chairman." The role includes planning and organizing peaceful, lawful demonstrations. Cindy wants to continue providing the FBI with information about the group's possible criminal activities.
- (U//FOUO) **Analysis F:** Being selected to this position of authority within the organization while being a CHS for the FBI is UDP that may influence the activities of the organization or the exercise of First Amendment rights of its members. Therefore, prior review by OGC is required before tasking her. OGC would conclude that Cindy's role as activities chairman would likely influence the activities of the organization. Additional facts would be needed to determine whether Cindy's activities may influence the exercise of the members' First Amendment rights. The operational AD would be able to approve the UDP if First Amendment rights are not likely to be impacted. However, if the facts indicate that Cindy may affect or have a pivotal role in the group's decision making process when determining how, when or where it will exercise First Amendment rights, OGC would conclude that Cindy's new role is likely to have an influence on the First Amendment rights of members of the organization. This determination would require review by the SORC and approval by the Director.
- G) (U//FOUO) **Example G:** An international terrorism Type 3 Assessment is opened seeking information about the connections John may have to those who are associated with supporting terrorist organizations. There is intelligence reporting that John meets with Paul at a local church where he (Paul) solicits funds from church members to support an organization that is affiliated with terrorism. The case agent tasks a CHS to attend a religious service that is open to the public to see if John is meeting with Paul. The CHS is tasked to attend up to 5 times over the course of 3 months but never sees John at these services. The agent now wants to task a different CHS to attend the next five services to see if he can observe John meeting with Paul.
- (U//FOUO) **Analysis G:** The attendance by the first CHS at five religious services open to the public is not considered UDP. Passive attendance on five occasions or less (see footnote #8 above) by a person who is not a member of the organization is not considered "participation" in the affairs of the organization for UDP purposes. However, the "Special Rule for Religious Services" requires the agent to obtain the prior approval of the SAC because the CHS was tasked to attend the religious service during an Assessment (SSA approval is required for Predicated Investigations).
- (U//FOUO) If the agent tasked the first CHS to attend more than five services or take an active role while attending those services, it would require sensitive UDP approvals, i.e., review by the CDC, approval by the SAC, and notice to the SORC. The agent does not avoid the UDP requirements by tasking a different CHS to perform the same task (looking for John to meet with Paul) for an additional five services.
- (U//FOUO) Even if the tasking of the second CHS were for a different purpose and part of a different Assessment or Predicated Investigation, ongoing or long-term attendance at a religious service may give the appearance that the FBI is monitoring First Amendment-protected activity. In these circumstances, employees should consult with their supervisor and the CDC or OGC as to whether additional review or approval is appropriate.
- H) (U//FOUO) **Example H:** A local non-affiliated church holds Sunday services open to the public in a strip mall. Other businesses in the strip mall include a gun dealer and an "army-navy store" selling survival equipment and military-style clothing. The minister who preaches at the Sunday service is also the owner of the "army-navy store." The FBI receives a tip that on the following Sunday a noted survivalist, who is also a major in the Freedom Militia, a

predicated domestic terrorist group, will be speaking at the church. The Major is a predicated subject in another investigation. What approvals are needed to task a CHS to attend the service at which the Major will speak?

(U//FOUO) **Analysis H:** The CHS is not a regular attendee and is only being tasked to attend a single service for the purpose of trying to locate an FBI subject. The CHS's attendance under these circumstances would not be considered "participation" for purposes of UDP. As set forth in section 16.2.3.C, passive "infrequent attendance" (see footnote #8 above) at a religious service that is open to the public (five occasions or less) by a person who is not a member of the organization does not constitute "participation." Because the CHS is being "tasked" to attend a religious service, however, the Special Rule for Religious Services would apply. (See DIOG Section 18.5.1.3.1) In an Assessment, the SAC must approve "tasking" a CHS to attend a religious service. In a Predicated Investigation, SSA approval is required.

- I) (U//FOUO) **Example I:** In the course of a Predicated Investigation into whether certain leaders of a mosque are recruiting members to travel to Pakistan to obtain training at Al Qaeda training camps, a CHS is tasked to join the mosque. The CHS is directed not to participate in any private meetings with the Imam or any other officials of the mosque. He is directed only to report on information that is generally known to members of the mosque.

(U//FOUO) **Analysis I:** This is a sensitive UDP because it entails joining a religious organization. Because the CHS has been tasked to join the mosque and report information he learns, review by the CDC and prior approval by the SAC are required. If approved, the field office must notify the SORC within 10 days following this approval.

- J) (U//FOUO) **Example J:** Later in the investigation, information is developed that the Imam and other members of the mosque are holding private meetings to discuss raising funds to be remitted to Hamas. The case agent wants to task the CHS to ingratiate himself with these individuals in the hopes that he will be invited to attend those private meetings.

(U//FOUO) **Analysis J:** Because this is a Predicated Investigation, no additional approvals are required in addition to the SAC approval already given. If this were an Assessment and the CHS were being tasked in the same way, review by OGC and approval by the responsible Assistant Director, with notice to the SORC, would be required.

- K) (U//FOUO) **Example K:** In the same investigation, the CHS has been asked to join the Board of Directors of the mosque. There is no intent to influence First Amendment rights. If, however, the CHS is a member of the Board of Directors, simply by voting or discussing items on the Board's agenda, it is likely that First Amendment rights will be affected.

(U//FOUO) **Analysis K:** OGC and SORC review and approval by the Director are required. In deciding whether to approve, the Director will consider whether this level of UDP is necessary to meet a significant investigative goal that cannot be achieved without the UDP.

- L) (U//FOUO) **Example L:** In the course of a predicated counterintelligence investigation, a UCE portrays herself as a college student. Consistent with her cover, she registers for classes on-line but does not actually attend any classes, take on-line classes, or use an email account affiliated with the college.

(U//FOUO) **Analysis L:** This does not constitute UDP because simply registering for university classes does not constitute participation in the university's activities. If the UCE attends any classes or takes an on-line class, sensitive UDP approvals would need to be obtained.

- M) (U//FOUO) **Example M:** A Predicated Investigation is being conducted regarding a recognized and approved university fraternity that is alleged to be involved in drug activity.

An Agent has developed a CHS (not a student), who has become friendly with one of the fraternity members and the member has invited the CHS to come to the fraternity and participate in fraternity activities. The Agent tasks the CHS to participate in the fraternity activities and obtain information about the drug activity at the fraternity. The Agent obtains any necessary OIA approvals.

(U//FOUO) **Analysis M:** This is a sensitive UDP because it involves undisclosed participation in an organization having an academic nexus (e.g., a student association). Even though the CHS is not a student, he is being tasked to participate in the activities of this organization having an academic nexus. Since the CHS has been tasked to participate in and obtain information about fraternity activities, review by the CDC and prior approval by the SAC are required. If UDP is approved, the field office must notify the SORC within 10 days.

17 (U) OTHERWISE ILLEGAL ACTIVITY (OIA)

17.1 (U) OVERVIEW

(U//FOUO) Otherwise Illegal Activity (OIA) is conduct in the course of duties by an FBI employee (to include an undercover employee (UCE)) or a confidential human source (CHS) which constitutes a crime under local, state, or federal law if engaged in by a person acting without authorization. OIA can be authorized for an FBI employee or CHS to obtain information or evidence necessary for the success of an investigation under the following limited circumstances: (i) when that information or evidence is not reasonably available without participation in the OIA; (ii) when necessary to establish or maintain credibility of cover identity in an undercover or covert investigation; or (iii) when necessary to prevent serious bodily injury or death. Certain types of OIA cannot be authorized, such as participation in conduct that would constitute an unlawful investigative technique (e.g., an illegal wiretap) or participation in an act of violence. In this context, "participation in an act of violence" does not include acts taken in self-defense and defense of others by the FBI employee or CHS because such actions would not be illegal.

17.2 (U) PURPOSE AND SCOPE

(U//FOUO) The use of OIA may be approved in the course of undercover activities or operations that involve an FBI employee or that involve use of a CHS. When approved, OIA should be limited or minimized in scope to only that which is reasonably necessary under the circumstances including the duration and geographic area to which approval applies, if appropriate.

17.3 (U//FOUO) OIA IN UNDERCOVER ACTIVITY

(U//FOUO) *General*: The use of the undercover method is discussed in the DIOG Section 18.6.13. OIA is often proposed as part of an undercover scenario or in making the initial undercover contacts before the operation is approved. Specific approval for OIA must be obtained in the context of these undercover activities or operations in addition to general approval of the scenario or the operation.

(U//FOUO) OIA by an FBI employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence: must be approved in conformity with *The Attorney General's Guidelines on FBI Undercover Operations* (AGG-UCO). Approval of OIA in conformity with the AGG-UCO is sufficient and satisfies any approval requirement that would otherwise apply under the AGG-Dom. Additional discussion is provided in the Field Guide for FBI Undercover and Sensitive Operations. A Special Agent in Charge (SAC) may approve the OIA described in subsection 17.5.

- A) (U//FOUO) When a UCE provides goods and service (reasonably unavailable to the subject except as provided by the United States government) that facilitate a felony, or its equivalent under federal, state, or local law, it is a sensitive circumstance. In these sensitive

circumstances, additional authorization by an Assistant Director is required after review by the Criminal Undercover Operations Review Committee (CUORC).

- B) (U//FOUO) Participation in otherwise illegal activity that involves a significant risk of violence or physical injury requires authorization by the Director, Deputy Director, or designated Executive Assistant Director after review by the CUORC.

(U//FOUO) OIA by an FBI employee in an undercover operation (UCO) relating to a threat to the national security or foreign intelligence collection must conform to the AGG-Dom and the FBI's National Security Undercover Operations Policy Implementation Guide (NSUCOPG). The Department of Justice (DOJ) National Security Division (NSD) is the approving component for OIA that requires approval beyond that authorized for SAC approval described in DIOG subsection 17.5, below. However, as authorized by the Assistant Attorney General for NSD, officials in other DOJ components may approve OIA in such investigations.

17.4 (U//FOUO) OIA BY A CONFIDENTIAL HUMAN SOURCE (CHS)

(U//FOUO) OIA by a CHS must be approved in conformity with the AGG-CHS and the FBI CHSPG.

17.5 (U//FOUO) APPROVAL OF OIA BY A SPECIAL AGENT IN CHARGE (SAC) – NOT INCLUDING MATERIAL SUPPORT OF TERRORISM

(U//FOUO) An SAC may authorize the following OIA for an FBI employee when consistent with other requirements of this section, the AGG-Dom, the AGG-UCO, and other FBI policy unless otherwise indicated. Except for subsections A, B, and E below, the following OIA activities require CDC review prior to SAC approval, unless otherwise indicated:

- A) (U//FOUO) Otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
- B) (U//FOUO) Consensual monitoring, even if a crime under state, local, or tribal law;
 - 1) (U//FOUO) Consent of all parties to the communication: For those state, local and tribal governments that require all parties to a conversation to consent to monitoring and do not sanction or provide a law enforcement exception for one-party consent recording of communications with persons within their jurisdiction, prior SAC approval for this OIA is required. This OIA approval authority is delegable to an Assistant Special Agent in Charge (ASAC) or Supervisory Special Agent (SSA). In most situations, the SAC of the employee who is seeking to conduct the consensual monitoring will be the approving official for this OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.
 - a) (U//FOUO) The law of the state or territory where the monitoring will take place will govern whether OIA approval is needed.
 - b) (U//FOUO) Consensual monitoring authority and OIA in states that require the consent of all-parties to the communication with no law enforcement exception for FBI employees and non-confidential parties may be authorized for the duration of the investigation, unless specified otherwise, and appropriately documented. As noted in subsection 17.4 above, OIA authority for a CHS can only be approved for 90 day periods, as set forth in the AGG-CHS and the FBI CHSPG. Consensual monitoring OIA for CHS must be renewed every 90 days.

- c) (U//FOUO) See the OGC website for a list of those states that require consent of all parties to the communication and do not have a law enforcement exception.
- 2) (U//FOUO) *FBI employee and non-confidential party (OIA)*: When consensual monitoring will be conducted by an FBI employee or a non-confidential party where the consent of all parties to the communication is required and there is no law enforcement exception for the FBI, the OIA approval must be obtained from the SAC of the employee who is seeking to conduct the consensual monitoring and documented in a properly executed FD-759. The FD-759 must be filed in the appropriate ELSUR subfile. This approval authority is delegable to an ASAC or SSA. Such OIA approval may be granted for the duration of the investigation, as long as the consensual monitoring circumstances do not materially change.
- 3) (U//FOUO) *CHS (OIA)*: When consensual monitoring will be conducted by a CHS in a state or territory where the consent of all parties to the communication is required and there is no law enforcement exception for the FBI, the OIA approval must be obtained from the SAC of the field office where the CHS is handled. This approval authority is delegable to an ASAC or SSA. The initial OIA approval for consensual monitoring must be documented in a properly executed FD-759. Such OIA approval may be granted for a maximum of 90 days, with no additional OIA documentation required for monitoring during that period. If it is necessary to extend the OIA for consensual monitoring beyond the initial 90-day period, another FD-759 may be used or, alternatively, such OIA for consensual monitoring may be requested, approved, and documented with an EC consistent with the AGG-CHS and CHSPG.
- 4) (U//FOUO) Other approvals for the consensual monitoring may apply such as those required when the consensual monitoring involves a sensitive monitoring circumstance. See DIOG Section 18.6.1.6.3.
- C) (U//FOUO) The controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
- D) (U//FOUO) The payment of bribes;
- (U//FOUO) *Note*: the payment of bribes and the amount of such bribes in a public corruption matter may be limited by other FBI policy (see the Public Corruption PG and Confidential Funding PG);
- E) (U//FOUO) The making of false representations in concealment of personal identity or the true ownership of a proprietary; and
- F) (U//FOUO) Conducting a money laundering transaction or transactions involving an aggregate amount not exceeding \$1 million.

(U//FOUO) The field office should notify the appropriate FBIHQ operational division and OGC of any OIA proposed activity that in the judgment of the approving official may expose employees or others to significant personal safety risks, create a risk of civil liability, result in adverse publicity, or raise any other sensitive operational concern. As a matter of FBI policy, "judgment" means that the decision of the authorizing official is discretionary.

(U//FOUO) An SAC may not authorize a violation of export control laws or laws that concern the proliferation of weapons of mass destruction during an investigation relating to a threat to the national security or foreign intelligence collection.

17.6 (U//FOUO) OIA RELATED TO MATERIAL SUPPORT OF TERRORISM IN NATIONAL SECURITY INVESTIGATIONS

(U//FOUO) In accordance with Part V.C.3 of the AGG-Dom, the Director of the FBI and the Assistant Attorney General for the NSD of the DOJ established the following policy concerning OIA as it relates to material support of terrorism in national security investigations (see EC dated 01/16/2009, 319W-HQ-A1487699-OGC Serial 35).

- A) (U//FOUO) If funds, items, or services that will be provided to a subject as part of a national security investigation may constitute material support to terrorism, an FBI, AD, with oral approval from the NSD, DOJ, may authorize the provision of such funds, items, or services if their value does not exceed \$2,000 per transaction and \$10,000 per operation per year. The preceding sentence applies only if the goods or services are available to the general public and if the AD reasonably believes that the funds, items or services will not be used to pose an imminent significant threat to any individual.
- B) (U//FOUO) NSD has represented that, except in exceptional circumstances, NSD shall act upon such an oral request within 24 hours and shall, within 72 hours, provide the FBI documentation of the authorization, including any terms and conditions.
- C) (U//FOUO) Any request and approval must be consistent with the terms and conditions of any license or non-objection agreement provided by the Office of Foreign Assets Control, Department of the Treasury, the Department of State, or the Department of Commerce.
- D) (U//FOUO) Except in exceptional circumstances, any request for approval of OIA that may constitute material support to terrorism, other than those described in paragraph A, must be made in writing to NSD.

(U//FOUO) Any questions about this policy or its implementation should be directed to OGC, National Security Law Branch, Counterterrorism Law Units.

17.7 (U//FOUO) STANDARDS FOR REVIEW AND APPROVAL OF OIA

(U//FOUO) No official may recommend or approve participation by an FBI employee in OIA unless the participation is justified:

- A) (U//FOUO) To obtain information or evidence necessary for the success of the investigation and not reasonably available without participation in the otherwise illegal activity;
- B) (U//FOUO) To establish or maintain credibility of a cover identity; or
- C) (U//FOUO) To prevent death or serious bodily injury.

17.8 (U) OIA NOT AUTHORIZED

(U//FOUO) The following activities may not be authorized as OIA:

- A) (U//FOUO) Directing or participating in acts of violence;

(U//FOUO) Note: Self-defense and defense of others. FBI employees are authorized to engage in any lawful use of force, including the use of force in self-defense or defense of others in the lawful discharge of their duties.

- B) (U//FOUO) Activities or investigative methods that cannot be authorized because they are prohibited by law, including activities that would violate protected constitutional or federal statutory rights in the absence of a court order or warrant such as illegal wiretaps and searches. For example, approving a non-consensual, non-emergency wiretap without a court order; approving the search of a home without a warrant or an exception to the warrant requirement, etc.

17.9 (U) EMERGENCY SITUATIONS

(U//FOUO) Without prior approval, an FBI employee may engage in OIA that could be authorized under this section only if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a situation, prior to engaging in the OIA, every effort should be made by the FBI employee to consult with the SAC, and by the SAC to consult with the United States Attorney's Office (USAO) or appropriate DOJ Division where the authorization of that office or division would be required unless the circumstances preclude such consultation. Circumstances in which OIA occur pursuant to this paragraph without the authorization required must be reported as soon as possible to the SAC, and by the SAC to FBIHQ and to the USAO or appropriate DOJ Division.

18 (U) INVESTIGATIVE METHODS

18.1 (U) OVERVIEW

18.1.1 (U) INVESTIGATIVE METHODS LISTED BY SUB-SECTION NUMBER

(U) The following investigative methods are listed by DIOG Sub-Section number:

18.5.1 (U) Public information.

18.5.2 (U) Records or information - FBI and DOJ.

18.5.3 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.

18.5.4 (U) On-line services and resources.

18.5.5 (U) CHS use and recruitment.

18.5.6 (U) Interview or request information from the public or private entities.

18.5.7 (U) Information voluntarily provided by governmental or private entities.

18.5.8 (U) Physical Surveillance (not requiring a court order).

18.5.9 (U) Grand jury subpoenas – for telephone or electronic mail subscriber information only.

18.6.1 (U) Consensual monitoring of communications, including electronic communications.

18.6.2 (U) Intercepting the communications of a computer trespasser.

18.6.3 (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices.

18.6.4 (U) Administrative subpoenas.

18.6.5 (U) Grand jury subpoenas.

18.6.6 (U) National Security Letters.

18.6.7 (U) FISA Order for business records.

18.6.8 (U) Stored wire and electronic communications and transactional records.

18.6.9 (U) Pen registers and trap/trace devices.

18.6.10 (U) Mail covers.

18.6.11 (U) Polygraph examinations.

18.6.12 (U) Searches – without a warrant or court order.

18.6.13 (U) Undercover operations.

18.7.1 (U) Searches – with a warrant or court order.

18.7.2 (U) Electronic surveillance – Title III.

18.7.3 (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information).

18.1.2 (U) INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)

(U) The following investigative methods are listed alphabetized by DIOG name:

(U) Administrative subpoenas. (Section 18.6.4)

(U) CHS use and recruitment. (Section 18.5.5)

(U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section 18.6.3)

(U) Consensual monitoring of communications, including electronic communications. (Section 18.6.1)

(U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (Section 18.7.3)

(U) Electronic surveillance – Title III. (Section 18.7.2)

(U) FISA Order for business records. (Section 18.6.7)

(U) Grand jury subpoenas. (Section 18.6.5)

(U) Grand jury subpoenas – for telephone or electronic mail subscriber information only in Type 1 & 2 Assessments. (Section 18.5.9)

(U) Information voluntarily provided by governmental or private entities. (Section 18.5.7)

(U) Intercepting the communications of a computer trespasser. (Section 18.6.2)

(U) Interview or request information from the public or private entities. (Section 18.5.6)

(U) Mail covers. (Section 18.6.10)

(U) National Security Letters. (Section 18.6.6)

(U) On-line services and resources. (Section 18.5.4)

(U) Pen registers and trap/trace devices. (Section 18.6.9)

(U) Physical Surveillance (not requiring a court order). (Section 18.5.8)

(U) Polygraph examinations. (Section 18.6.11)

(U) Public information. (Section 18.5.1)

(U) Records or information - FBI and DOJ. (Section 18.5.2)

(U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section 18.5.3)

(U) Searches – without a warrant or court order. (Section 18.6.12)

(U) Searches – with a warrant or court order. (Section 18.7.1)

(U) Stored wire and electronic communications and transactional records. (Section 18.6.8)

(U) Undercover Operations. (Section 18.6.13)

18.1.3 (U) GENERAL OVERVIEW

(U//FOUO) The conduct of Assessments, Predicated Investigations (Preliminary Investigations and Full Investigations) and other activities authorized by the Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) may present choices between the use of different investigative methods (formerly investigative "techniques") that are each reasonable and effective based upon the circumstances of the investigation, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and the potential damage to reputation. The least intrusive method if reasonable based upon the circumstances of the investigation is to be used in such situations. However, the choice of methods is a matter of judgment. The FBI is authorized to use any lawful method consistent with the AGG-Dom, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of the foreign intelligence sought to the United States' interests. (AGG-Dom, Part I.C.2.)

(U) The availability of a particular investigative method in a particular investigation may depend upon the level of investigative activity (Assessment, Preliminary Investigation, Full Investigation, and Assistance to Other Agencies).

18.2 (U) LEAST INTRUSIVE METHOD

(U) The AGG-Dom requires that the "least intrusive" means or method be considered and—if reasonable based upon the circumstances of the investigation—used to obtain intelligence or evidence in lieu of more intrusive methods. This principle is also reflected in Executive Order 12333, which governs the activities of the United States intelligence community (USIC). The concept of least intrusive method applies to the collection of intelligence and evidence.

(U) Selection of the least intrusive means is a balancing test as to which FBI employees must use common sense and sound judgment to effectively execute their duties while mitigating the potential negative impact on the privacy and civil liberties of all people encompassed within the Assessment or Predicated Investigation, including targets, witnesses, and victims. This principle is not intended to discourage investigators from seeking relevant and necessary intelligence, information, or evidence, but rather is intended to encourage investigators to choose the least

intrusive—yet still reasonable —means from the available options to obtain the material. Additionally, FBI employees should operate openly and consensually with United States persons (USPERs) to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

(U) DIOG Section 4.4 describes the least intrusive methods concept and the standards to be applied by FBI employees.

18.3 (U) PARTICULAR INVESTIGATIVE METHODS

(U//FOUO) All lawful investigative methods may be used in activities under the AGG-Dom as authorized by the AGG-Dom. Lawful investigative methods include those investigative methods contained in this DIOG as well as additional investigative methods and resources authorized in other FBI policy and guidance (for example, future additions to DIOG Sections 18, as well as Policy Implementation Guides). In some instances the authorized investigative methods are subject to special restrictions or review or approval requirements. (AGG-Dom, Part V.A.)

18.3.1 (U) USE OF CRIMINAL INVESTIGATIVE METHODS IN NATIONAL SECURITY INVESTIGATIONS

(U//FOUO) Because national security investigations may implicate criminal issues as well, the availability of criminal investigative methods should be considered when appropriate. However, any use of criminal investigative methods should be closely coordinated with FBIHQ, both operational units and the NSLB, prior to any anticipated use of this criminal investigative process. The NSLB maintains liaison with DOJ OI respecting the use of FISA authorized investigative methods in national security investigations.

18.4 (U) INFORMATION OR EVIDENCE OBTAINED IN ASSESSMENTS AND PREDICATED INVESTIGATIONS

(U) The use, retention and/or dissemination of information obtained during authorized investigations must comply with the AGG-Dom and the DIOG. If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

During the course of an Assessment or Predicated Investigation, FBI employees lawfully may actively or passively receive items of evidence or intelligence from a variety of sources. It has been demonstrated that the relevance of every item of evidence or intelligence received is not always apparent at the time it is obtained. Accordingly, FBI employees are given latitude to establish or determine the relevance of information as the investigation develops. Nevertheless, as a matter of administrative efficiency and to protect the privacy of the individual, if an FBI employee obtains an item of evidence which clearly is not relevant to the investigation and there is no foreseeable future evidentiary or intelligence value to the FBI or the USIC, the item should be returned or destroyed. The disposition of the item should be documented in the file or on the FD-713.

or Guardian (FD-71a). In the alternative, such item of evidence may be sequestered in the investigative file. If it is later determined that the item of evidence is relevant, the item may be used in the investigation upon such determination. The determination of relevancy will be made on a case-by-case basis with supervisory direction and may include consultation with the appropriate federal prosecuting office and/or the Chief Division Counsel (CDC) or the Office of the General Counsel (OGC). This policy does not supersede Sections 18.6.4.1.5 (Administrative Subpoenas); 18.6.5.1 (Federal Grand Jury Subpoena); 18.6.6.1.7 (National Security Letters); or 18.6.7.1.6 (FISA Order for Business Records), or any requirement imposed by statute, regulation or other applicable law.

18.5 (U) AUTHORIZED INVESTIGATIVE METHODS IN ASSESSMENTS

(U) See AGG-Dom, Part II.A.4.

(U//FOUO) An FBI employee must document on the FD-71 or in Guardian, the use of or the request and approval for the use of authorized investigative methods in Type 1 & 2 Assessments. Certain Type 1 & 2 Assessment situations may require the use of an EC to document the use and approval of certain investigative methods. All authorized investigative methods in Type 3, 4, and 6 Assessments must use an EC to document the use of or the request and approval for the use of the applicable investigative method. See DIOG Section 5.6.3.4 for the investigative methods authorized in a Type 5 Assessment.

(U) In conducting an Assessment, only the following investigative methods are authorized:

- A) (U) Public information. (See Section 18.5.1)
- B) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
- C) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
- D) (U) On-line services and resources. (See Section 18.5.4)
- E) (U) CHS use and recruitment. (See Section 18.5.5)
- F) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
- G) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
- H) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- I) (U//FOUO) Grand jury subpoenas - for telephone or electronic mail subscriber information only (during a Type 1 & 2 Assessment) (See Sections 18.5.9 and 18.6.5)

(U//FOUO) In Assessments, supervisory approval is required prior to use of the following investigative methods: certain interviews, tasking of a CHS, and physical surveillance not requiring a court order. During Predicated Investigations, supervisory approval requirements for these investigative methods may not apply.

This Page is Intentionally Blank.

18.5.1 (U) INVESTIGATIVE METHOD: PUBLIC INFORMATION (“PUBLICLY AVAILABLE INFORMATION”)

(U) See AGG-Dom, Part II.A.4.a and Part VII.L.

18.5.1.1 (U) SCOPE

(U//FOUO) Public information is “Publicly Available Information” that is:

- A) (U) Published or broadcast for public consumption;
- B) (U) Available on request to the public;
- C) (U) Accessible on-line or otherwise to the public;
- D) (U) Available to the public by subscription or purchase;
- E) (U) Made available at a meeting open to the public;
- F) (U) Obtained by visiting any place or attending an event that is open to the public (e.g., public places); or
- G) (U) Observed, heard, smelled, detected or obtained by any casual observer or member of the public and does not involve unconsented intrusion into private places.

(U//FOUO) The phrase “observed, heard, smelled, detected or obtained by any casual observer or member of the public” includes, for example, plain view observations; overhearing a conversation taking place at an adjacent table in a public restaurant; odor detection (by a person, drug dog, or technical device) emanating from a vehicle, in a public place, or from locations to which the employee has gained lawful access; searching property that has been intentionally abandoned, including property discarded in public trash containers or common dumpsters (but does not include a “trash cover” as set forth in DIOG Section 18.6.12).

(U//FOUO) The following are examples:

- 1) (U) Viewing the vehicle identification number or personal property that is exposed to public view and may be seen when looking through the window of a car that is parked in an area that is open to and accessible by members of the public;
- 2) (U) The examination of books and magazines in a book store or the purchase of such items. See *Maryland v. Macon*, 472 U.S. 463 (1985); and
- 3) (U) A deliberate overflight in navigable air space to photograph marijuana plants is not a search, despite the landowner’s subjective expectation of privacy. See *California v. Ciraolo*, 476 U.S. 207 (1986).

(U//FOUO) **Note:** Consent Searches are authorized in Assessments, as well as in Predicated Investigations.

(U//FOUO) **Note:** If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.1.2 (U) APPLICATION

(U//FOUO) This investigative method may be used prior to opening an Assessment, in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies.

18.5.1.3 (U) APPROVAL

(U//FOUO) Supervisory approval is not required for use of this method, except for the special rule for attending a religious service, even if it is open to the public. (See DIOG Section 18.5.1.3.1)

18.5.1.3.1 (U//FOUO) SPECIAL RULES: "SPECIAL RULE FOR RELIGIOUS SERVICES" AND "SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS"**18.5.1.3.1.1 (U//FOUO) SPECIAL RULE FOR RELIGIOUS SERVICES – REGARDLESS OF WHETHER IT IS OPEN TO THE GENERAL PUBLIC**

- A) (U//FOUO) In Assessments: Tasking a CHS to attend a religious service requires SAC approval, which cannot be delegated. An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16). Undercover activity is not permitted during an Assessment.
- B) (U//FOUO) In Predicated Investigations: Tasking a CHS to attend a religious service requires SSA approval. An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) or if attendance is part of an undercover operation (see DIOG Section 18.6.13).

18.5.1.3.1.2 (U//FOUO) SPECIAL RULE FOR OTHER SENSITIVE ORGANIZATIONS

- A) (U//FOUO) In Assessments: Tasking a CHS to attend an event or activity of a sensitive organization as defined in DIOG Section 16.1.3, other than a public gathering that includes substantial numbers of individuals who are not members of the organization (e.g., a public rally; a conference to which the public is invited and is expected to attend), requires SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16). Undercover activity is not permitted during an Assessment.
- B) (U//FOUO) In Predicated Investigations: No supervisory approval is required. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) or if attendance is part of an undercover operation (see DIOG Section 18.6.13).

18.5.1.4 (U) USE/DISSEMINATION

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

18.5.2 (U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – FBI AND DEPARTMENT OF JUSTICE (DOJ)

(U) See AGG-Dom, Part II.A.4.b.

18.5.2.1 (U) SCOPE

(U//FOUO) An FBI employee may access and examine FBI and other DOJ records and may obtain information from any FBI personnel or other DOJ personnel. Access to certain FBI records may be restricted to designated FBI personnel because of the sensitive nature of the information in the record, the classification of the record, or the tool used to gather the information contained in the record. These include, but are not limited to: FBI records concerning human source identification; espionage investigations; code word; other compartmented information; records that include raw FISA collections; and Rule 6(e) material.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.2.2 (U) APPLICATION

(U//FOUO) This investigative method may be used prior to opening an Assessment, in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies.

18.5.2.3 (U) APPROVAL

(U//FOUO) Supervisory approval is not required to use this method, except that if the use of records constitutes pattern-based data mining under the Federal Data Mining Reporting Act of 2007, it must be reviewed and approved according to Section 18.5.2.4 below.

18.5.2.4 (U) PATTERN-BASED DATA MINING

(U//FOUO) As used here, pattern-based data mining (PBDM) means queries or other analysis of electronic databases using two or more search criteria designed to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals (as defined in Corporate Policy Directive 0310D). Any such analysis based solely on racial, ethnic, national origin or religious characteristics is strictly prohibited.

(U//FOUO) For purposes of this requirement, pattern-based data mining does not include activities using one or more personal identifiers to identify an individual or analysis designed to discover links between a specific subject and unknown individuals or entities, even if the subject's actual identity is not yet known. Pattern-based data mining does not include queries or analysis designed solely to identify potential human sources of intelligence nor does it include activities designed to identify an individual or individuals associated with criminal or terrorist activity that has already occurred. For example, database queries using multiple criteria to identify foreign visitors to the United States of a certain age and gender from

specific foreign countries who may engage in espionage is pattern-based data mining within the meaning of the statute. In contrast, database queries using criteria such as a physical description and motor vehicle owned to identify possible suspects in a kidnapping do not constitute pattern-based data mining, because the queries are being used to investigate a crime that has already occurred. Queries designed to identify individuals or entities who have had contact with a specific individual are not pattern-based data mining; rather, such queries are subject-based data mining, even if the specific individual's actual identity is presently unknown.

(U//FOUO) The majority of data analysis performed during FBI Assessments and Predicated Investigations is based on specific individuals or events and therefore does not constitute pattern-based data mining because it is either link analysis or is not predictive of future behavior.

(U//FOUO) A Privacy Threshold Analysis (PTA) for pattern-based data mining must be completed and forwarded to the Privacy and Civil Liberties Unit, OGC. See the OGC Privacy PG for additional details.

(U//FOUO) The Sensitive Operations Review Committee (SORC) must also receive notice of any proposal to use pattern-based data mining as defined above. Additionally, pursuant to the Federal Agency Data Mining Reporting Act of 2007,¹¹ the FBI must advise the DOJ of all agency initiatives that involve the use of PBMD, so that those activities may be included in the Department's annual report to Congress. (See CPD 0310D, "Pattern-based Data Mining Reporting Requirements").

18.5.2.5 (U) Use/Dissemination

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

(U//FOUO) The request for the records and the records received from DOJ and used during an Assessment or Predicated Investigation must be maintained as part of the appropriate file (e.g., 801 et. seq classification file, zero sub-assessment file, or investigation file).

¹¹ (U) 42 U.S.C. § 2000ee-3

18.5.3 (U) INVESTIGATIVE METHOD: RECORDS OR INFORMATION – OTHER FEDERAL, STATE, LOCAL, TRIBAL, OR FOREIGN GOVERNMENT AGENCY

(U) See AGG-Dom, Part II.A.4.c.

18.5.3.1 (U) SCOPE

(U//FOUO) An FBI employee may access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies. When requesting information using this authority, care must be taken to ensure the entity to which the request is made understands that it is not compelled to provide such information or create a new record to assist the FBI.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.3.2 (U) APPLICATION

18.5.3.3 (U//FOUO) This investigative method may be used prior to opening an Assessment, in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies. (U) Approval

(U//FOUO) Supervisory approval is not required to use this method for “routine uses,” unless such approval is required by Memoranda of Understanding (MOU) or other agreements for requesting such information.

(U//FOUO) **Requests to other Federal Agencies:** The FBI may request another federal agency to disclose Privacy Act-protected records pursuant to the other agency’s “routine uses” (5 U.S.C. § 522a[b][3]) or through a written request for a law enforcement purpose (5 U.S.C. § 522a[b][7]). Such written requests (for a law enforcement purpose) pursuant to 5 U.S.C. § 522a(b)(7) may be made by the Director or his designee, provided that such authority may not be delegated below the Section Chief level (28 C.F.R. § 16.40[c]; OMB Guidelines, 40 Fed. Reg. at 28,955). Pursuant to these provisions, the Director hereby delegates his authority to request from federal agencies information and records otherwise protected from disclosure by the Privacy Act, at FBIHQ, to all Section Chiefs and above, and in the field, to all SACs and ADICs. This authority may not be redelegated to a person below the rank of SAC in the field and SC in FBIHQ.

(U//FOUO) **Requests to Foreign Agencies:** Requests for records or information from a foreign government entity or agency must be appropriately coordinated through the applicable FBI Legat office, International Operations Division (IOD), INTERPOL, relevant FBIHQ operational division, and/or DOJ Office of International Affairs, as necessary. Direct contact with foreign government agencies is authorized in certain circumstances, such as an imminent threat situation.

(U//FOUO) If the analysis of records obtained in this manner constitutes PBMD under the Federal Data Mining Reporting Act of 2007, it must be reviewed and approved according to Section 18.5.2.3, above.

(U//FOUO) *Example:* An MOU at a local fusion center or a joint task force may specify procedures for the FBI to follow when requesting records or information from state and local governmental entities or agencies.

18.5.3.4 (U) Use/Dissemination

(U//FOUO) The use and/or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

(U//FOUO) The request for the records and the records received from an outside entity and used during an Assessment or Predicated Investigation must be maintained as part of the appropriate file (e.g., 801 et. seq classification file, zero sub-assessment file, or investigation file).

18.5.4 (U) INVESTIGATIVE METHOD: ON-LINE SERVICES AND RESOURCES

(U) See AGG-Dom, Part II.A.4.d.

18.5.4.1 (U) SCOPE

(U//FOUO) An FBI employee may use any publicly available on-line service or resource including those that the FBI has obtained by subscription or purchase for official use, including services available only to law enforcement entities.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.4.2 (U) APPLICATION

(U//FOUO) This investigative method may be used prior to opening an Assessment, in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies.

18.5.4.3 (U) APPROVAL

(U//FOUO) Supervisory approval is not required to use this method, although subscribing to or purchasing any new service or resource must be done according to FBI contracting procedures.

(U//FOUO) *Example:* Publicly available on-line services or resources include, but are not limited to: Google, Yahoo, or similar Internet search services. Online resources that may be purchased by the FBI for official use include, but are not limited to: data brokers such as ChoicePoint, Westlaw, and Lexis-Nexis; and vehicle, casualty, and property insurance claims databases such as Claim-Search.

18.5.4.4 (U) USE/DISSEMINATION

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

(U) See DIOG Appendix L – On-line Investigations for additional information.

This Page is Intentionally Blank.

18.5.5 (U) INVESTIGATIVE METHOD: CHS USE AND RECRUITMENT

(U) See AGG-Dom, Part II.A.4.e.

18.5.5.1 (U) SCOPE

(U//FOUO) The FBI may use and recruit human sources in Assessments and Predicated Investigations in conformity with the AGG-Dom, Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources (AGG-CHS), the FBI Confidential Human Source Program Guide (CHSPG), and the FBI Confidential Human Source Validation Source Manual (CHSVSM). In this context, “use” means obtaining information from, tasking, or otherwise operating such sources. See AGG-Dom, Part VII.V.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.5.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2.

(U) When collecting positive foreign intelligence, the FBI must operate openly and consensually with an USPER, to the extent practicable.

(U//FOUO) A CHS can be “used” in support of an Assessment and a Predicated Investigation or for the purpose of validating, vetting or determining the suitability of another CHS as part of an Assessment.

18.5.5.3 (U) APPROVALS

(U//FOUO) All investigative methods should be evaluated to ensure compliance with the admonition that the FBI should use the least intrusive method if reasonable based upon the circumstances of the investigation. That requirement should be particularly observed during an Assessment when using a CHS because the use of a CHS during an Assessment may be more intrusive than many other investigative methods. Use of a CHS in an Assessment should take place only after considering whether there are effective, less intrusive means available to obtain the desired information. The CHS must comply with all constitutional, statutory, and regulatory restrictions and limitations. In addition:

- A) (U//FOUO) CHS use and direction must be limited in focus and scope to what is necessary to accomplish the authorized purpose and objective of the Assessment or Predicated Investigation. The FBI employee's tasking of the CHS, to include the focus and scope, must be included in the FBI employee's report contained in DELTA.
- B) (U//FOUO) During an Assessment, a CHS may be directed to seek information about an individual, group or organization (see the Special Rule for Religious Services and the Special Rule for Other Sensitive Organizations below) only to the extent that such information is

necessary to achieve the specific objective of the Assessment. If such contact reveals information or facts about an individual, group or organization that meets the requirements to open a Predicated Investigation, a Predicated Investigation may be opened, as appropriate.

C) (U//FOUO) **Special Rule for Religious Services** – regardless of whether it is open to the general public:

- 1) (U//FOUO) **In Assessments**: Tasking a CHS to attend a religious service requires SAC approval, which cannot be delegated. An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16). Undercover activity is not permitted during an Assessment.

(U//FOUO) **In Predicated Investigations**: Tasking a CHS to attend a religious service requires SSA approval. An FBI employee attending a religious service overtly must have SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) or if attendance is part of an undercover operation (see DIOG Section 18.6.13).

D) (U//FOUO) **Special Rule for Other Sensitive Organizations**:

- 1) (U//FOUO) **In Assessments**: Tasking a CHS to attend an event or activity of a sensitive organization as defined in DIOG Section 16.1.3, other than a public gathering that includes substantial numbers of individuals who are not members of the organization (e.g., a public rally; a conference to which the public is invited and is expected to attend), requires SSA approval. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16). Undercover activity is not permitted during an Assessment.
- 2) (U//FOUO) **In Predicated Investigations**: No supervisory approval is required. Higher approvals may be required under certain circumstances, such as attendance that rises to the level of UDP (see DIOG Section 16) or if attendance is part of an undercover operation (see DIOG Section 18.6.13).

E) (U//FOUO) **Public Information**: If the CHS is not tasked to join or participate in the activities of a legitimate organization (which must be approved in accordance with DIOG Section 16), tasking a CHS to find publicly available information or to reveal non-confidential information to which the CHS already has access may be done without supervisory approval in an Assessment or Predicated Investigation.

F) (U//FOUO) **Non-Public Information**: Tasking a CHS to join or actively participate in the activities of a legitimate group or organization, including those in which the CHS is already a member or participating, for the purpose of obtaining information that is not publicly available from or about the organization requires approval as “Undisclosed Participation” (UDP), as discussed in Section 16. During an Assessment, a CHS should not be so tasked unless the information cannot be obtained through less intrusive means and the information is necessary to the Assessment. Furthermore, depending on the nature of the group or organization, such tasking may involve a First Amendment protected activity and trigger higher approval levels. See DIOG Section 16.

G) (U//FOUO) A CHS cannot be tasked to do that which an FBI employee cannot legally do. Thus, for example, if a subpoena or court order is required to obtain certain information, such as bank records or credit reports, a CHS cannot be tasked to obtain such information. This principle does not, however, eliminate the legal concept of a consent search or the doctrine of misplaced confidence. The doctrine of misplaced confidence provides that a person assumes

the risk when dealing with a third party that the third party might be a government agent and might breach the person's confidence. Thus, by way of example, although the government would be required to have a search warrant to enter a person's premises involuntarily to ascertain whether the premises are being used to facilitate criminal conduct, the FBI is permitted to task a CHS to gain the owner's confidence so that the CHS can enter the premises based on an invitation from the owner to ascertain whether the premises are being so used.

- H) (U//FOUO) If there is any conflict between the CHSPG, CHSVSM or any other PG and the DIOG, the DIOG controls. OGC, OIC and CPO should be immediately notified of any such conflict.

18.5.5.4 (U) Use/Dissemination

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom, DIOG Section 14, and the CHSPG.

This Page is Intentionally Blank.

18.5.6 (U) INVESTIGATIVE METHOD: INTERVIEW OR REQUEST INFORMATION FROM THE PUBLIC OR PRIVATE ENTITIES

(U) See AGG-Dom, Part II.A.4.f; AGG-Dom, Part II.B.4.

18.5.6.1 (U) SCOPE

(U//FOUO) An interview is the questioning of an individual (to include a subject) in order to gather information that is pertinent to and within the scope of an authorized Assessment or Predicated Investigation. The initial questioning of a complainant is not an interview, nor is re-contacting a complainant to clarify information that was initially provided. Normally, an FBI employee should disclose the employee's affiliation with the FBI and true purpose of the interview at the outset. The person being interviewed is voluntarily providing information and his/her Constitutional rights must be respected. FBI employees may not obtain a statement by force, threats, or improper promises. FBI employees have no authority to promise leniency or immunity from prosecution. Additionally, the interviewer should make reasonable efforts to obtain information that is accurate, relevant, timely, and complete. An interview may only elicit a description of how an individual exercises a right guaranteed by the First Amendment to the Constitution if such information is pertinent to and within the scope of an authorized activity; similarly, regardless of how such information is elicited, it may not be maintained in FBI files unless it is pertinent to and within the scope of an authorized activity.

(U//FOUO) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property.

(U//FOUO) *Note:* Consent Searches" are authorized in Assessments, as well as in Predicated Investigations.

(U//FOUO) *Note:* If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.6.2 (U) APPLICATION

(U//FOUO) Interviews may be used prior to opening an Assessment, in Assessments, Predicated Investigations, assistance to other agencies, when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. FBI employees must not use any interview technique that is in violation of the DIOG, the AGG-Dom or is abusive or coercive, regardless of whether a co-interviewer is in compliance with his/her agency's guidelines.

18.5.6.3 (U) VOLUNTARINESS

(U//FOUO) Information that is sought during an interview must be provided voluntarily. FBI employees may not obtain a statement by force, threats, or improper promises. FBI employees have no authority to promise leniency or immunity from prosecution. If, during a non-custodial interview, the interviewee indicates he or she wishes to consult an attorney, the interviewer should assess whether continuing the interview would negatively affect the voluntariness of any further information provided. In determining whether a statement has

been given voluntarily, courts evaluate a “totality of the circumstances,” which may include consideration of the following factors:

- A) (U//FOUO) Whether the interviewee was notified of any charges against him/her or advised of his/her rights;
- B) (U//FOUO) The interviewee’s age, intelligence, experience, and physical condition;
- C) (U//FOUO) Whether there was any physical abuse or threats of abuse during the interview;
- D) (U//FOUO) The number of officers present and whether weapons were displayed during the interview;
- E) (U//FOUO) Whether threats or psychological pressure was used during the interview;
- F) (U//FOUO) Whether the interviewee was deprived of food, sleep, medication, or outside communication during the interview;
- G) (U//FOUO) The duration of the interview, and whether any trickery, ruse, or deception was used; and
- H) (U//FOUO) Whether there were any promises of leniency or other inducements made during the interview.

(U//FOUO) See Sections 18.5.6.3.8, 18.5.6.3.9, and 18.5.6.4.13 below for additional considerations when interviewing juveniles.

(U//FOUO) These factors are illustrative. The presence of any one or more of the factors mentioned above will not necessarily make a statement involuntary.

18.5.6.4 (U) APPROVAL / PROCEDURES

(U) With the exceptions discussed below, interviews do not require supervisory approval.

18.5.6.4.1 (U) CUSTODIAL INTERVIEWS

(U//FOUO) An FBI employee must advise a person who is in custody of his/her *Miranda* rights, per form FD-395, before beginning an interview inside the United States with the exception of questioning reasonably prompted by a concern for public safety (discussed below). It is critical that the person understand his/her rights before questioning. By signing the FD-395, the defendant acknowledges that he/she has been advised of his/her rights and is willing to proceed without a lawyer present.

(U//FOUO) A person is “in custody” for purposes of *Miranda* when his/her freedom of movement is significantly restricted. Custody can arise short of formal arrest when, judging from the totality of the circumstances, a reasonable person in the position of the interviewee would believe that he/she is in custody. A brief, temporary investigative detention is not custody provided it is reasonable in scope. In assessing whether a temporary detention is reasonable in scope and thus not custody for purposes of *Miranda*, factors to consider include the degree of force used to affect the detention, use of restraining devices and whether the individual was moved from the location of the stop. Employees can clarify custodial status by telling the person that he/she is not under arrest.

18.5.6.4.1.1 (U) MIRANDA WARNINGS REQUIRED

(U//FOUO) *Miranda* warnings are required when a person:

- A) (U//FOUO) Has been arrested and is in federal, tribal, state, or local custody;
- B) (U//FOUO) Is significantly restricted in his freedom of movement to a degree normally associated with a formal arrest; or
- C) (U//FOUO) Regardless of custody, has previously been formally charged, prosecution is pending, and the subject matter of the interview concerns the pending charge.

(U//FOUO) For the purposes of *Miranda*, an interview refers to express questioning and any words or actions that are reasonably likely to elicit an incriminating response. In a custodial interview, the individual must be advised of the names and official identities of the employee(s) conducting the interview, the nature of the inquiry, and provided *Miranda* warnings, per the FD-395 form, before being interviewed. After being advised of his/her rights, if an interviewee who is in custody, invokes the right to counsel and/or the right to remain silent, this must be honored and the interview must cease. However, once the advice of rights is provided and it is evident that the interviewee understood those rights, the interview may proceed until such time as the interviewee invokes a right. While an affirmative waiver, including signing a waiver portion of the FD-395 is preferred, it is not required. Once the interviewee invokes his/or her right to remain silent and/or right to counsel, the interview must immediately be terminated. The fact that the interviewee invoked the right to counsel and/or the right to remain silent should be recorded on the FD-395 and the form should be executed in all other respects.

18.5.6.4.1.2 (U) MIRANDA WARNINGS NOT REQUIRED

(U//FOUO) There are certain custodial interviews in which the protection *Miranda* provides against self-incrimination may not be served by reading the standard warnings and obtaining a waiver. In the following circumstances, *Miranda* warnings are not required for custodial interviews:

- A) (U//FOUO) standard booking questions;
- B) (U//FOUO) an interview of the incarcerated individual as a victim or witness in an unrelated matter that does not pertain to any pending charges against the interviewee;
- C) (U//FOUO) the public safety exception (discussed in more detail below); and
- D) (U//FOUO) in connection with arrests of operational terrorists inside the United States (discussed in more detail below).

18.5.6.4.1.3 (U//FOUO) PUBLIC SAFETY EXCEPTION

(U//FOUO) The warning and waiver of rights is not required when questions are asked that are reasonably prompted by a concern for public safety. For example, if Agents make an arrest in public shortly after the commission of an armed offense, and need to make an immediate inquiry to determine the location of the weapon, such questions may be asked, even of an in-custody suspect, without first advising the suspect of the warnings contained in Form FD-395. This public safety exception could also apply to other

situations where imminent threat(s) to the safety of law enforcement officers or member(s) of the public could be alleviated by questions necessary to neutralize the threat.

18.5.6.4.1.4 (U//FOUO) ADVICE OF RIGHTS IN CONNECTION WITH ARRESTS OF OPERATIONAL TERRORISTS INSIDE THE UNITED STATES¹²

(U//FOUO) Identifying and apprehending suspected terrorists, interrogating them to obtain intelligence about terrorist activities and impending terrorist attacks, and lawfully detaining them so that they do not pose a continuing threat to our communities are critical to protecting the American people. The DOJ and the FBI believe that we can maximize our ability to accomplish these objectives by continuing to adhere to FBI policy regarding the use of *Miranda* warnings for custodial interrogation of operational terrorists¹³ who are arrested inside the United States:

- A) (U//FOUO) If applicable, agents should ask any and all questions that are reasonably prompted by an immediate concern for the safety of the public or the arresting agents without advising the arrestee of his *Miranda* rights.¹⁴
- B) (U//FOUO) After all applicable public safety questions have been exhausted, agents should advise the arrestee of his/her *Miranda* rights and seek a waiver of those rights before any further interrogation occurs, absent the exceptional circumstances described below.
- C) (U//FOUO) There may be exceptional cases in which, although all relevant public safety questions have been asked, agents nonetheless conclude that continued unwarned interrogation is necessary to collect valuable and timely intelligence not related to any immediate threat, and that the government's interest in obtaining this intelligence outweighs the disadvantages of proceeding with unwarned interrogation.¹⁵

¹² (U//FOUO) This guidance applies only to arrestees who have not been indicted and who are not known to be represented by an attorney. For policy concerning the interrogation of indicted defendants, see Section 18.5.6.4.1; and for policy concerning contact with represented persons, see DIOG Section 18.5.6.4.5.

¹³ (U//FOUO) For these purposes, an operational terrorist is an arrestee who is reasonably believed to be either a high-level member of an international terrorist group; or an operative who has personally conducted or attempted to conduct a terrorist operation that involved risk to life; or an individual knowledgeable about operational details of a pending terrorist operation.

¹⁴ (U//FOUO) The Supreme Court held in *New York v. Quarles*, 467 U.S. 649 (1984), that if law enforcement officials engage in custodial interrogation of an individual that is "reasonably prompted by a concern for the public safety," any statements the individual provides in the course of such interrogation shall not be inadmissible in any criminal proceeding on the basis that the warnings described in *Miranda v. Arizona*, 384 U.S. 436 (1966), were not provided. The Court noted that this exception to the *Miranda* rule is a narrow one and that "in each case it will be circumscribed by the {public safety} exigency which justifies it." 467 U.S. at 657.

¹⁵ (U//FOUO) The Supreme Court has strongly suggested that an arrestee's Fifth Amendment right against self-incrimination is not violated at the time a statement is taken without *Miranda* warnings, but instead may be violated only if and when the government introduces an unwarned statement in a criminal proceeding against the defendant. See *Chavez v. Martinez*, 538 U.S. 760, 769 (2003) (plurality op.); *id.* at 789 (Kennedy, J., concurring in part and dissenting in part); *cf. also id.* at 778-79 (Souter, J., concurring in the judgment); See also *United States v. Patane*, 542 U.S. 630, 641 (2004) (plurality opinion) ("[V]iolations [of the Fifth Amendment right against self-incrimination] occur, if at all, only upon the admission of unwarned statements into evidence at trial."); *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("[A] violation [of the Fifth Amendment right against self-incrimination] occurs only at trial.").

(U//FOUO) In these exceptional cases, agents must seek SAC approval, which cannot be delegated, to proceed with an unwarned interrogation after the public safety questioning is concluded. The SAC must consult with FBIHQ (including OGC) and DOJ attorneys before granting approval. Presentment of an arrestee may not be delayed simply to continue the interrogation, unless the arrestee has timely waived prompt presentment.

(U//FOUO) The determination whether particular unwarned questions are justified on public safety grounds must always be made on a case-by-case basis based on all the facts and circumstances. In light of the magnitude and complexity of the threat often posed by terrorist organizations, particularly international terrorist organizations, and the nature of their attacks, the circumstances surrounding an arrest of an operational terrorist may warrant significantly more extensive public safety interrogation without *Miranda* warnings than would be permissible in an ordinary criminal investigation. Depending on the facts, such interrogation might include, for example, questions about possible impending or coordinated terrorist attacks; the location, nature, and threat posed by weapons that might pose an imminent danger to the public; and the identities, locations, and activities or intentions of accomplices who may be plotting additional imminent attacks.

(U//FOUO) As noted above, if there is time to consult with FBIHQ (including OGC) and Department of Justice attorneys regarding the interrogation strategy to be followed prior to reading the arrestee his *Miranda* rights, the field office should endeavor to do so. Nevertheless, the agents on the scene who are interacting with the arrestee are in the best position to assess what questions are necessary to secure their safety and the safety of the public, and how long the post-arrest interview can practically be delayed while interrogation strategy is being discussed.

18.5.6.4.2 (U//FOUO) MIRANDA WARNINGS FOR SUSPECTS IN CUSTODY OVERSEAS

(U//FOUO) The decision to use or not use *Miranda* warnings during an overseas custodial interrogation will have to be made on a case by case basis and weigh many factors. Overall, if there is a reasonable likelihood of a prosecution in a U.S. civilian criminal court of the person being interrogated while in custody overseas, agents should discuss with FBIHQ, FBI OGC, and DOJ whether warnings should be provided to the person being interrogated. Once the determination is made to provide *Miranda* warnings as part of an overseas custodial interrogation, if the person being interrogated invokes his right to remain silent or consult with an attorney, this invocation should be honored. If use of *Miranda* warnings is appropriate given the circumstances of the case, the following DOJ-approved modified waiver form should be used. The form is the Standard Advice of Rights for Suspects in Foreign Custody.

18.5.6.4.3 (U) CONSTITUTIONAL RIGHTS TO SILENCE AND COUNSEL UNDER MIRANDA

- A) (U//FOUO) **Silence:** If a custodial interviewee invokes his/her right to remain silent, FBI employees should not attempt a subsequent interview until a significant period of time has elapsed (a two-hour period has been held to be significant) or the interviewee requests to be interviewed anew. In either case, an FBI employee will ensure that the interviewee is again advised of his/her *Miranda* rights and indicates that he/she understand those rights before further questioning. If the interviewee again asserts his/her right to remain silent or the right to counsel, questioning must cease at that time. Assertion of the right to silence, like assertion of

the right to counsel, must be unequivocal and unambiguous. A waiver of the right to remain silent occurs when an interviewee knowingly and voluntarily makes a statement; assertion of the right to remain silent requires more than mere silence in the face of questioning. This right, like the right to counsel, can be invoked at any time during custodial interrogation. Agents may continue questioning someone who has not clearly invoked his/her right to remain silent, but if the custodial interviewee asserts his/her right to silence, questioning must cease at that time.

- B) (U//FOUO) **Counsel:** If a custodial interviewee invokes his/her right to counsel, questioning must cease. FBI employees may not attempt a subsequent interview unless counsel is present, the custodial interviewee initiates contact, or there has been a break in custody of at least 14 days.
- 1) (U//FOUO) When a custodial interviewee who has invoked his/her right to counsel initiates a subsequent interview, an FBI employee must ensure that the interviewee is advised of and understands his/her *Miranda* rights before proceeding with the interview. Not every statement by a custodial interviewee can fairly be interpreted as initiating a subsequent interview. In order to constitute the initiation of an interview, the custodial interviewee must either directly request such or use words that are reasonably interpreted as expressing a desire to be interviewed. If the words used are ambiguous, the FBI employee should clarify the custodial interviewee's intent by asking directly whether the custodial interviewee wants to be interviewed. The words and responses, if any, to such clarifying questions should be documented. General conversation by a custodial interviewee cannot be interpreted as indicating a desire to be interviewed and cannot be used standing alone to predicate a second interview after the right to counsel has been invoked. If the interviewee again asserts his/her right to counsel, or invokes his/her right to silence, questioning must cease at that time.
 - 2) (U//FOUO) When an uncharged and/or unrepresented interviewee who has previously invoked his/her right to counsel experiences a break-in-custody of at least 14 days, he/she may be approached for a subsequent interview. FBI employees, however, must ensure that the custodial interviewee is again advised of and waives his/her *Miranda* rights before proceeding with the interview. A break-in-custody for these purposes can occur even if an interviewee is continuously incarcerated. Questions as to what constitutes a break-in-custody should be directed to the CDC or OGC.
 - 3) (U//FOUO) Contact with a represented person outside the presence of his/her counsel may implicate state ethics rules for attorneys (AUSAs). Before making such contact, employees are encouraged to contact the CDC, OGC, or the USAO. Once a represented person has been charged, information may only be elicited from the person: 1) regarding an unrelated or uncharged matter or 2) when counsel is present. Questions as to whether an individual is in fact represented or may be questioned as to a particular matter should be directed to the CDC or OGC.

18.5.6.4.4 (U) SIXTH AMENDMENT RIGHT TO COUNSEL

(U//FOUO) The Sixth Amendment Right to Counsel requires the government to advise and obtain a waiver of the Right to Counsel prior to interviewing the person to whom the right has attached. The Right to Counsel attaches upon indictment regardless of whether the indicted person realizes an indictment has been returned. The Right to Counsel also attaches upon the filing of information and at the time of an initial appearance on a Federal Complaint. The Right to Counsel is offense specific. When applicable, a warning regarding the Right to

Counsel and subsequent knowing and voluntary waiver must occur prior to an interview, regardless of whether the person is in custody. Providing a person with a *Miranda* warning and obtaining a waiver per the use of Form FD-395 will permit the interview of the person after the Right to Counsel has attached. The Sixth Amendment right to counsel does not prohibit the government from re-contacting the subject if the subject refuses initially to waive this right or otherwise has requested or obtained counsel following an Initial Appearance. However, further attempts to interview the subject may be prohibited if the subject invoked his right to counsel and remained in continuous custody or there was an insufficient break in custody (consistent with *Miranda* and its progeny). In addition, due to concerns associated with contact with represented persons (See 18.5.6.4.5), guidance from the CDC or OGC should be obtained before contact is made with a subject who has obtained or requested counsel if the contact relates to the crime charged and the subject's counsel has not been notified.

18.5.6.4.5 (U) CONTACT WITH REPRESENTED PERSONS

(U//FOUO) CDC or OGC review is required before contact with represented persons in the absence of prior notice to counsel. Such contact may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the CDC must follow applicable law and DOJ procedure when reviewing the request to contact the represented individual in the absence of prior notice to counsel. The SAC, CDC, or their designees, and the United States Attorney or his or her designees must consult periodically on applicable law and DOJ procedure relative to contact with represented persons. The field office may raise inconsistent application of: (i) state ethics rules; or (ii) rules for contacts with represented persons with the USAO and request that it consult with the DOJ Professional Responsibility Advisory Office. (AGG-Dom, Part V.B.1)

18.5.6.4.6 (U) MEMBERS OF THE UNITED STATES CONGRESS AND THEIR STAFFS

(U//FOUO) Generally, FBI employees may accept information offered from Congressional offices just as they would accept information from other sources, and they may act upon it accordingly. SAC and appropriate FBIHQ AD approval, and prior notice to the AD Office of Congressional Affairs (OCA), are required if an employee seeks to: (i) establish an informant relationship with a Member of Congress or with Congressional staff; (ii) interview a Member of Congress or Congressional staff in connection with a public corruption matter; or (iii) interview a Member of Congress or Congressional staff in connection with a foreign counterintelligence matter. The FBIHQ operational division policy implementation guides (PGs) may contain additional notice requirements.

18.5.6.4.7 (U) WHITE HOUSE PERSONNEL

(U//FOUO) FBI employees may accept information offered by White House personnel just as they would accept information from other sources, and they may act upon it accordingly. SAC and appropriate FBIHQ AD approval, after consultation with OGC, is, however, required before initiating contact with White House personnel as part of an investigation. SAC and AD approval (from the appropriate operational division), after consultation with OGC, is also required if an employee seeks to establish an informant relationship with any member of the

White House staff. Additional guidance regarding contact with White House personnel may be found in the AG Memorandum captioned "Communications with White House and Congress" dated May 11, 2009. (See DIOG Appendix D) Note: The FBIHQ operational division PGs may contain additional notice requirements for conducting interviews or seeking an informant relationship with White House personnel. In addition personnel assigned to the Washington Field Office may, after OGC approval, obtain authority to contact White House personnel on routine investigations where White House personnel may have been a victim or witness.

18.5.6.4.8 (U) MEMBERS OF THE NEWS MEDIA

18.5.6.4.8.1 (U) APPROVAL REQUIREMENTS

18.5.6.4.8.1.1 (U) GENERAL REQUIREMENTS

(U//FOUO) Attorney General approval must be obtained prior to conducting an interview of a member of the news media for any offense which the member of the news media is suspected of having committed in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of his/her official duties as a member of the news media. Requests for this approval must be submitted with an EC to the AD of the operational FBIHQ division that is responsible for the investigative classification and the AD of the Office of Public Affairs (OPA). The requesting EC must be reviewed by the CDC and approved by the SAC after coordinating the request with the local USAO. The EC must contain the necessary facts and investigative justification for the interview consistent with the DOJ guidelines set forth in 28 C.F.R. § 50.10.

18.5.6.4.8.1.2 (U) EMERGENCY CIRCUMSTANCES REQUIREMENTS

(U//FOUO) In emergency circumstances, an Agent may interview a news media representative concerning an offense which the member of the news media is suspected of having committed in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of his/her official duties as a member of the news media without prior AG approval, if authorized by the SAC and the United States Attorney. Immediate notification of the interview, the emergency circumstances that justified proceeding without prior authorization and all the information that would have been provided if prior authorization had been sought shall be communicated immediately to the AD of the FBIHQ operational division, the AD of the OPA, and the General Counsel. The AD of the operational division is responsible for notifying the appropriate officials at DOJ as set forth in 28 C.F.R. 50.10. After these oral notifications have been made, the field office is responsible for providing written documentation to the FBIHQ operational division AD as soon as practicable, but not more than 24 hours after the interview. FBIHQ is responsible for providing appropriate written documentation to the DOJ approval authorities to whom oral notice was given.

18.5.6.4.8.2 (U) USE OF SUBTERFUGE

(U//FOUO) To the extent operational needs allow, investigators must operate openly and consensually with members of the news media. If an interview of a member of the news media involves any subterfuge (whether the purpose of the interview is related to the news gathering circumstances set forth in the preceding paragraph or otherwise), the interview and the subterfuge must be approved by the AD of the operational division responsible for the investigation. The EC requesting permission must include the facts and circumstances surrounding the interview, including an explanation why the investigator cannot operate openly and consensually with the news media person to be interviewed. Additionally, the EC must include a description of the planned subterfuge. After consultation with the OPA and OGC, the AD of the operational division must decide whether to approve the request. If the request requires approval by DOJ (because the interview is related to an offense committed by the member of the news media during the course of news gathering) the AD of the operational division is responsible for submitting all requests for approval to the DOJ per 28 C.F.R. 50.10.

(U//FOUO) FBIHQ operational division PGs may contain additional notice requirements.

18.5.6.4.9 (U) DURING AN ASSESSMENT - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST

- A) (U//FOUO) In the normal course of an interview, an FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview. FBI employees must operate openly and consensually with members of the public during an Assessment unless operational considerations preclude the disclosure of true affiliation or purpose, in which case, employees must adhere to the policies listed below.
- B) (U//FOUO) During an Assessment, an FBI employee may request information without disclosing the true purpose of the request provided that the false purpose would not reasonably be expected to violate the rights or damage the reputation of another person and provided the false purpose does not imply that adverse legal consequences may follow if the interviewee declines to speak to the FBI employee.
- C) (U//FOUO) Undercover activity is not authorized during an Assessment. "Undercover activity" includes the use of false identity to obtain intelligence or evidence from a subject or other person of interest.
- D) (U//FOUO) An FBI employee is not required to affirmatively disclose his or her FBI affiliation if non-disclosure is reasonably necessary to achieve the purpose of the Assessment and the FBI employee is:
 - 1) (U//FOUO) Attending a public event or place (including presence in publicly accessible on-line space or venue) on the same terms as a member of the general public;
 - 2) (U//FOUO) Present at a public event or place (including a publicly accessible on-line space or venue) and the employee is invited to engage in a limited follow-on conversation with a third party outside of the public event or place (or online space or venue);
 - 3) (U//FOUO) Engaged in incidental contact or interaction with members of the public or private entities;
 - 4) (U//FOUO) Engaged in limited interaction to protect cover;

- 5) (U//FOUO) Tacitly representing him or herself as an associate of another law enforcement officer;
- 6) (U//FOUO) Engaged in a properly authorized Type 5 Assessment; or
- 7) (U//FOUO) Engaged in limited interaction with a third party.

(U//FOUO) For each circumstance above, an employee's FBI affiliation should only be withheld if doing so is not reasonably expected to adversely affect the rights or damage the reputation of another person or to have reasonably anticipated legal consequence.

(U//FOUO) In a Type 5 Assessment to vet a potential source, alias/false identity documentation (AFID) may be used for the limited purpose of vetting a potential source if done in accordance with the CHSPG. AFID may not be used with the intent to collect, or with the expectation of collecting, intelligence or evidence through conversations with a subject or other person of interest—as this activity may constitute undercover activity.

(U//FOUO) The authority to withhold disclosure of FBI affiliation does not extend to an interview seeking intelligence or evidence material to an Assessment. Conducting an interview without disclosing FBI affiliation may constitute undercover activity, which is prohibited in an Assessment. If FBI affiliation has been withheld and intelligence or evidence has been revealed unexpectedly, the FBI employee may continue to receive information voluntarily provided by the other party. The FBI employee must document and report the circumstances to a supervisor at the earliest opportunity.

18.5.6.4.10 (U) CONSULTATION AND DISCUSSION

(U//FOUO) The authorities granted above to engage members of the public without disclosing the true purpose of the request and to engage in limited interaction with the public without affirmatively disclosing FBI affiliation are intended to provide an effective, efficient, and timely means to resolve Assessments. At the same time, this policy is designed to prevent inadvertent noncompliance with the prohibition on undercover activity during an Assessment by, for example, using a false identity (including Alias False Identification (AFID)) to conduct an interview seeking intelligence or evidence during an Assessment. There will not always be a bright line between undercover activity and authorized interaction with the public in some operational scenarios. FBI employees are strongly encouraged to consult with the CDC or OGC when questions arise regarding use of this section. During an Assessment, if there is any doubt about whether the plan constitutes undercover activity, the FBI should not proceed with the plan.

18.5.6.4.11 (U) EXAMPLES

18.5.6.4.11.1 (U) EXAMPLE 1

(U//FOUO) During an Assessment, for the purpose of conducting limited surveillance, an agent attends a motorcycle rally open to the public without disclosing his FBI affiliation. On arrival, the agent is asked to show some ID and sign in. May the agent produce a false driver's license and sign in under an alias?

(U//FOUO) Answer: Yes, this limited interaction and use of AFID is permitted in this circumstance to protect the agent's cover.

18.5.6.4.11.2 (U) EXAMPLE 2

(U//FOUO) During an Assessment, an agent seeks to learn whether a particular individual still resides in a particular dangerous neighborhood. She plans to wear a UPS shirt and carry a clipboard into an apartment building and knock on some doors asking if the individual has moved from the building. May the agent proceed in this manner?

(U//FOUO) Answer: Yes, this constitutes engaging in limited interaction with a third party. Although the agent intends to have contact with members of the public, her interaction is limited and not designed to obtain information regarding the third party.

18.5.6.4.11.3 (U) EXAMPLE 3

(U//FOUO) During an Assessment, an agent surveilling a subject follows the subject into an office building. The building security requires everyone entering to sign in but does not check ID. The surveillance agent is asked to sign a register, does so using a false name, and continues the surveillance. May the agent do this?

(U//FOUO) Answer: Yes, this is a good example of engaging in incidental contact to protect cover. It could also be considered incidental contact or interaction with members of the public or private entities.

18.5.6.4.11.4 (U) EXAMPLE 4

(U//FOUO) During an Assessment, an agent is seeking to determine the whereabouts of John Doe. The agent discloses his identity to one of Mr. Doe's neighbors and falsely tells the neighbor that he has reports that Doe was front and center in a crowd during which several foreign students were pelted with eggs and chided to leave the university campus because they were occupying seats that should go to taxpayers. The agent implies to the neighbor that it is very important to be able to establish that Doe was not, in fact, in the crowd. May the agent use this false statement of purpose?

(U//FOUO) Answer: No, this would damage the reputation of Doe in the neighborhood because it implies Doe was involved in criminal conduct.

18.5.6.4.11.5 (U) EXAMPLE 5

(U//FOUO) During a Type 5 Assessment, an agent calls a foreign student and tells the student she would like to discuss information contained on his visa. In fact, there is nothing about the student's visa of interest to the FBI; the agent's true purpose is to meet the student to assess him as a potential source. May the agent use that false statement of purpose in order to induce the student to meet and be interviewed?

(U//FOUO) Answer: Yes, the false purpose is permissible because it does not imply that legal consequences may follow if the student declines to speak to the agent. It would, however, not be permissible for the agent to tell the student that he has a serious visa

problem and could face deportation if he does not agree to meet with the agent, because that false purpose implies that adverse legal consequence will flow to the student if he declines to speak to the agent.

18.5.6.4.11.6 (U) EXAMPLE 6

(U//FOUO) The Joint Terrorism Task Force (JTTF) receives a Guardian lead stating that an employee of the East Side convenience store is a terrorist and that he has gone to Pakistan for terrorist training. The Guardian lead does not identify the alleged terrorist other than stating he works at the store. To resolve the lead, the agent first wants to determine who works at the store to see if the FBI has any intelligence that confirms or negates the lead. The agent conducts public records searches for the business. These are of limited value as they only provide the name of the owner of the business. Because the business is open 24 hours a day, there must be at least one additional employee. In order to resolve this possible threat quickly, the agent and a local police detective assigned to the JTTF obtain a photograph of a particularly disreputable looking task force officer to use in a ruse to determine who works at the business and whether anyone who works there has gone to Pakistan. The task force officer and the agent go to the business. The police officer identifies himself as a detective with the local police department and says that the agent is his partner. He explains to the man at the counter that there have been several robberies of local convenience stores of late (true on any given day) and that he would like the employee to look at the picture to see if he recognizes the person it depicts. The employee does not. Then, the task force officer asks for the name of other employees ostensibly so that he can also show them the picture. Can the agent proceed in this manner?

(U//FOUO) Answer: Yes, this a limited interaction with a third party who is not a subject or a person of interest and the agent is tacitly allowing himself to be held out as an associate of another law enforcement officer.

18.5.6.4.11.7 (U) EXAMPLE 7

(U//FOUO) An FBI agent accompanies a DHS Immigration and Customs Enforcement (ICE) agent task force member to check out an individual who has been detained incident to the individual's arrival into the United States at a border crossing. The individual is not known to be a subject in any ongoing investigation but acted in an unusual manner when asked at the border crossing about his country of origin. For operational reasons, the FBI agent does not wish to be identified as an FBI agent but instead will be introduced as the ICE agent's partner, falsely implying that she is also an ICE agent. May the FBI agent proceed to the immigration interview and allow the ICE agent to suggest that the FBI agent is an ICE agent?

(U//FOUO) Answer: Yes, the agent can tacitly represent herself to be associated with another law enforcement agency and may be present during the ICE interview. The agent may not, however, conduct the interview because doing so in a false affiliation capacity would be considered an "undercover activity."

18.5.6.4.11.8 (U) EXAMPLE 8

(U//FOUO) Continuing with these facts, shortly after arrival, during the visit an opportunity arises for an interview regarding smuggling of counterfeit cigarettes. The FBI agent is asked for her identification by the interviewee. May the agent respond by stating she is an ICE agent or by producing a false credential identifying her as such?

(U//FOUO) Answer: No, because this will be an interview that seeks intelligence or evidence. During an Assessment, the agent may not conduct an interview under an assumed identity as an ICE agent. She must either leave the interview or correctly identify herself as an FBI agent.

18.5.6.4.11.9 (U) EXAMPLE 9

(U//FOUO) As part of an authorized Assessment conducted online, an FBI employee visits a public chat forum using an Internet name that does not disclose FBI affiliation. The FBI employee engages an individual in discussion about another private forum where identity theft is discussed. This other forum is password protected and requires invitation from someone who is already a participant. The individual invites the FBI employee to access the forum and provides a password. May the FBI employee pursue the discussion in the private chat forum.

(U//FOUO) Answer: Yes, the FBI employee may engage in limited interaction outside the public forum based on an express invitation from someone who has access so long as there are no special rules apparent in releasing the password. Although limited interaction in a context like this is permissible, FBI employees must be very careful in such a scenario not to engage in undercover activity, which is not permitted during an Assessment.

18.5.6.4.12 (U//FOUO) PREDICATED INVESTIGATIONS - REQUESTING INFORMATION WITHOUT REVEALING FBI AFFILIATION OR THE TRUE PURPOSE OF A REQUEST

(U//FOUO) In the normal course of an interview, the FBI employee should divulge the employee's affiliation with the FBI and the true purpose of the interview. During a Predicated Investigation, however, an FBI employee may request information without revealing FBI affiliation or disclosing the true purpose of the request provided the false reason would not reasonably be expected to violate the rights or damage the reputation of another person or have reasonably anticipated legal consequence.

(U//FOUO) Withholding FBI affiliation may constitute undercover activity, e.g., when an employee uses an assumed identity to obtain intelligence or evidence from a subject or other person of interest. Undercover activity must comply with the guidelines contained in DIOG Section 18.6.13 and the AGG-UCO.

18.5.6.4.13 (U) INTERVIEWS OF JUVENILES

(U//FOUO) When determining whether to interview a juvenile (anyone under the age of eighteen) who does not fall within the provisions of the JDA above, e.g., when interviewing a

juvenile as a witness or subject prior to arrest, and, if so, determining the scope and tactics that will be used, the FBI employee should consider the age and competency of the juvenile, whether the juvenile is emancipated, the juvenile's relationship to the suspect(s), safety concerns, the gravity of the offense at issue, any alternative sources of evidence, the importance of the information or potential testimony to the investigation, and the juvenile's degree of involvement, if any, with the offense. If the interview is custodial, compliance with the provisions of the Juvenile Delinquency Act (JDA) below is necessary. In determining whether a juvenile is in custody the test remains an objective test – was there a formal arrest or a deprivation of freedom of movement equivalent to an arrest. However, with respect to juveniles, if the juvenile's age is known to the interviewer or is objectively apparent, the juvenile's age is to be considered in the custody analysis. This is not to say that age is the determining or decisive factor in every case, but it recognizes that age is to be considered given a reasonable adult may view the circumstances surrounding the interview differently than a reasonable juvenile. If the juvenile is placed under arrest, the procedures listed in 18.5.6.4.14 must be followed. If not under arrest, but based on the objective circumstances surrounding the interview, including the juvenile's age, the juvenile is deemed to be in custody, the interviewer should advise the juvenile of their rights as set forth in the FD-395 and cease the interview if the juvenile invokes a right. Parental consent for a juvenile interview should be obtained when feasible under the circumstances of the investigation.

- A) (U//FOUO) Special consideration should be given to child interviews and to interviews of juveniles who are of a tender age, maturity, or have a significant developmental disability. To the extent appropriate, agents should make use of local child protective services to aid in interviewing a child – especially for an offense involving sexual exploitation of the child. The agents should consider seeking approval to video and/or audio record child interviews to address potential allegations that the child was manipulated and to have an unimpeachable record in case the child's statement changes.
- B) U//FOUO) Federal statutes and the Attorney General Guidelines on Victim and Witness Assistance require federal investigators to utilize sensitive and developmentally appropriate practices designed to elicit the most accurate information from child victims and witnesses and to reduce unnecessary and additional trauma to these children. An interview should be appropriate for the age and developmental level of the child. It may be advisable in some instances for FBI employees to seek assistance with interviewing children – possibly by utilizing local child protective services – particularly, when the child is very young, developmentally disabled, or extremely traumatized. Interviews of child victims and witnesses, regardless of the type of crime, should be conducted by personnel properly trained in the techniques designed to best elicit accurate information from a child while minimizing additional trauma.

18.5.6.4.14 (U) INTERVIEWS OF JUVENILES AFTER ARREST

(U//FOUO) Under the Juvenile Delinquency Act (JDA), a juvenile is anyone who commits a federal crime before his or her eighteenth birthday and who has not yet reached age twenty-one (21) before being charged. The provisions of the JDA, 18 U.S.C. § 5031 *et seq.*, apply upon arrest.

- A) (U//FOUO) Whenever a juvenile is arrested for a violation of federal law, he/she must be immediately advised of his/her legal rights and the United States Attorney must be notified. The juvenile's parents, guardian or custodian must also be immediately notified of his/her

arrest as well as his/her rights and the nature of the alleged offense. After notification has been made, FBI employees must allow a parent, guardian, or custodian access to the juvenile if requested by the juvenile or by a parent, guardian or custodian of the juvenile. The juvenile must be promptly taken before a magistrate if a magistrate is available. If no magistrate is immediately available, the juvenile must be taken to a magistrate without undue delay.

- B) (U//FOUO) Whether a juvenile may be interviewed for a confession or admission of his own guilt between the time of his arrest for a federal offense and his initial appearance before the magistrate depends on the law of the circuit in which the arrest occurs. If the interrogation is not allowed under the law of the circuit, information volunteered by the arrested juvenile concerning his own guilt should be recorded in the FBI employee's notes for use in subsequent proceedings; clarifying questions may be asked as necessary to make certain the FBI employee correctly understands what the juvenile intends to say. The volunteered statement may be reduced to writing if such action does not involve any delay in the juvenile's appearance before the magistrate. Any questions concerning the law that applies in the particular circuit should be directed to the CDC.
- C) (U//FOUO) A juvenile may be questioned concerning the guilt of a third party if such questioning does not cause any delay in bringing him/her before the magistrate.
- D) (U//FOUO) These special requirements apply only after the arrest of a juvenile, as defined by federal law, for a federal offense. They do not apply when the juvenile is under arrest by state or local officers on a state or local charge but is suspected of having committed a federal offense. FBI employees may question a juvenile in custody on a non-federal charge about a federal offense for which he/she is a suspect. FBI employees are cautioned, however, that they may not collude or create the appearance of collusion with non-federal officers to delay an arrest on federal charges to circumvent the JDA requirements.
- E) (U//FOUO) A juvenile may waive his Fifth Amendment rights and consent to a post-arrest custodial interview if permitted by the law of the circuit. Whether a waiver is knowing and voluntary will be determined based on the totality of the circumstances surrounding the interview. Among the factors the court will likely consider are the juvenile's age, experience, education, background, and intelligence, and whether he/she has the capacity to understand the warnings given, the nature of Fifth Amendment rights, and the consequences of waiving them. The presence and co-signature of a parent or guardian during the waiver of rights (FD-395) is not required for a voluntary waiver, although it is a factor to be considered and might help dispel any notion that the juvenile was coerced. The AUSA must approve a post-arrest custodial interview of a juvenile.

18.5.6.4.15 (U) DOCUMENTATION

(U//FOUO) When it is anticipated that the results of an interview may become the subject of court testimony, the interview must be recorded on an FD-302 or FD-1023 (for debriefing of CHSs). The FD-302 or FD-1023 must contain a record of statements made by the interviewee. Analysis or contextual comments regarding an interviewee's statements should be documented in a companion EC or other appropriate format. If the interviewee characterizes an individual, group, or activity in a certain way, FBI records (i.e., 302s, ECs, LHMs) should reflect that the interviewee, not the FBI, is the source of the characterization.

(U//FOUO) Certain types of written material developed during the course of an interview must be retained including:

- A) (U//FOUO) Written statements signed by the witness. When possible, written statements should be taken in all investigations in which a confession or admission of guilt is obtained unless the confession is obtained during an electronically-recorded interview session. If a witness gives a signed statement, and then gives additional information orally, both the signed statement and the oral information should be recorded on an FD-302 or FD-1023;
- B) (U//FOUO) Written statements, unsigned by the witness, but approved or adopted in any manner by the witness. An example of such a written statement would be a written statement that the subject orally admits is true but will not sign; and
- C) (U//FOUO) Original notes of an interview when the results may become the subject of court testimony. Materials generated via email, text messages, or similar means during an online interview must be retained as original notes. Because some forms of synchronous communication tools, such as text messaging, have limited or no storage, print, or production capabilities, they should not be used for substantive communications with law enforcement colleagues or civilians who may become witnesses. **If these tools are, nonetheless, used for substantive communications as part of an interview, the communications must be memorialized verbatim in an FD-302.**
- D) (U//FOUO) If an FBI employee and an AUSA conduct an interview, and the AUSA asks or tells the FBI employee to refrain from recording the substance of the interview or taking notes, the FBI employee should decline to participate in the interview and should not be present when it takes place unless the interview is part of the trial preparation of the witness (or unless another law enforcement agent present is given the responsibility for taking notes and documenting the substance of the interview). FBI employees generally do not report the substance of trial preparation unless new material information or impeachment information is developed. FBI employees should consult with the trial AUSA to determine how to document any new information, including impeaching information, developed during the trial preparation interviews.

18.5.6.4.16 (U) ELECTRONIC RECORDING OF INTERVIEWS

(U//FOUO) Special Agents must obtain ASAC approval (which may not be delegated) prior to recording interviews. The requirement to obtain approval is not intended to discourage recording or to indicate that the FBI disfavors recording. Indeed, there are many circumstances in which audio or video recording of an interview may be prudent. Approval to electronically record an interview must be documented on a FD-759. When recording a custodial interview, the recording should include an advice and waiver of *Miranda* rights, as well as a question and answer segment designed to demonstrate that the interviewee's statements are voluntary and not the product of coercion.

(U//FOUO) After completing the recorded interview, the agent must document the fact that the interview took place in an FD-302, noting the identity of the individual recorded and the details of the recording session (e.g., date, time, start and stop periods, reasons for stopping). FBI employees may include a summary of the recording in the FD-302 if doing so will aid them in the management of the investigation. Transcription of the recording is optional.

(U//FOUO) Establishing within a field office reasonable standards for the types of investigations, crimes, circumstances, and subjects for which recording may be desirable will help maintain internal consistency. The following factors will assist the ASAC in determining whether to approve a request to record interview or interviews. These factors should not be

viewed as a checklist; they are not intended to limit the discretion of the approving official and are not intended to suggest that there is a presumption against recording.

- A) (U//FOUO) Whether the purpose of the interview is to gather evidence for prosecution, or intelligence for analysis, or both;
- B) (U//FOUO) If prosecution is anticipated, the type and seriousness of the crime, including, in particular, whether the crime has a mental element (such as knowledge or intent to defraud), proof of which would be considerably aided by the defendant's admissions in his own words;
- C) (U//FOUO) Whether the defendant's own words and appearance (in video recordings) would help rebut any doubt about the voluntariness of his confession raised by his age, mental state, educational level, or understanding of the English language; or is otherwise expected to be an issue at trial, such as to rebut an insanity defense; or may be of value to behavioral analysts;
- D) (U//FOUO) If investigators anticipate that the subject might be untruthful during an interview, whether a recording of the false statement would enhance the likelihood of charging and convicting the person for making a false statement;
- E) (U//FOUO) The sufficiency of other available evidence to prove the charge beyond a reasonable doubt;
- F) (U//FOUO) The preference of the USAO and the Federal District Court regarding recorded confessions;
- G) (U//FOUO) Local laws and practice--particularly in task force investigations where state prosecution is possible;
- H) (U//FOUO) Whether interviews with other subjects in the same or related investigations have been electronically recorded; and
- I) (U//FOUO) The potential to use the subject as a cooperating witness and the value of using his own words to elicit his cooperation.

18.5.6.4.17 (U) INTERVIEWS RELATING TO CLOSED FILES

(U//FOUO) An interview initiated by an employee should only be conducted if it is within the scope of an open authorized Assessment or Predicated Investigation. On the other hand, there are situations in which an individual contacts the FBI to report information concerning a matter that has been closed or placed in a zero file classification, or is unrelated to any current or previous investigation. In these situations, an FBI employee may collect whatever information the person is willing to provide, except solely First Amendment information, and may document the results of the contact in an FD-71/Guardian, or with an EC or FD-302. These documents may be uploaded in files that are relevant to an open Assessment or Predicated Investigation, a closed Assessment or Predicated Investigation, a zero classification file, or a control file (if no further investigative activity is required).

18.5.6.4.18 (U) FBIHQ OPERATIONAL DIVISION REQUIREMENTS

- A) (U//FOUO) *Counterintelligence Division*: Interviews conducted during counterintelligence Assessments and Predicated Investigations must comply with the requirements contained in the Memorandum of Understanding between the Department of State and the FBI on Liaison for Counterintelligence Investigations. The FBIHQ Counterintelligence Division PG contains interview approval requirements.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§18

B) (U//FOUO) Other FBIHQ Divisions: Each FBIHQ division may provide additional interview notice requirements in its PG.

18.5.6.5 (U) Use/Dissemination

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

**18.5.7 (U) INVESTIGATIVE METHOD: INFORMATION VOLUNTARILY PROVIDED BY
GOVERNMENTAL OR PRIVATE ENTITIES**

(U) See AGG-Dom, Part II.A.4.g.

18.5.7.1 (U) SCOPE

(U//FOUO) An FBI employee may accept information voluntarily provided by federal, state, local, tribal, or foreign governmental or private entities and individuals. Voluntarily provided information includes, but is not limited to, oral as well as documentary and physical evidence such as a computer hard drive or other electronic media that contains information, paper documents containing information, or physical objects (e.g., handgun or narcotics).

(U//FOUO) Nothing in this section prohibits asking for or accepting volunteered access to personal or real property.

(U//FOUO) **Note:** Consent Searches are authorized in Assessments, as well as Predicated Investigations.

(U//FOUO) **Note:** If the originator of information reported to the FBI characterizes an individual, group, or activity in a certain way, and that characterization should be documented for completeness of the FBI record, the FBI record (i.e., 302, EC, LHM) should reflect that another party, and not the FBI, is the originator of the characterization.

18.5.7.2 (U) APPLICATION

(U//FOUO) This investigative method may be used prior to opening an Assessment, in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3.

18.5.7.3 (U) APPROVAL

(U//FOUO) Supervisory approval is not required to accept voluntarily provided information. Personnel may not request nor knowingly accept information where disclosure would be prohibited by federal law. See, e.g., 18 U.S.C. § 2702 (prohibiting an entity providing electronic communications services from divulging certain communications and other records, except in certain circumstances).

18.5.7.4 (U) USE/DISSEMINATION

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

This Page is Intentionally Blank.

18.5.8 (U) INVESTIGATIVE METHOD: PHYSICAL SURVEILLANCE (NOT REQUIRING A COURT ORDER)

(U) See AGG-Dom, Part II.A.4.b – “Engage in observation or surveillance not requiring a court order.” *Note:* Consent Searches are authorized in Assessments.

(U) For additional information regarding physical surveillance during Assessments or predicated national security investigations, see DIOG Appendix G – Classified Provisions.

18.5.8.1 (U) SCOPE

(U//FOUO) ***Physical Surveillance Defined:*** Physical surveillance is the deliberate observation of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy.

(U//FOUO) ***Distinction between Casual Observation and Physical Surveillance:*** A bright line cannot be drawn between “casual observation” and “physical surveillance.” The distinction is necessarily determined by the facts and circumstances at hand. “Casual observation” should be short in duration and narrow in scope.

(U//FOUO) The following factors should be considered when determining whether a particular plan of action constitutes “casual observation,” for which there is no approval requirement, or “physical surveillance,” for which there may be approval requirements (see DIOG Section 18.5.8.2 below):

- A) (U//FOUO) The duration and frequency of the observation of a particular person or location. The longer or more frequent it is, the more likely it is physical surveillance;
- B) (U//FOUO) The location of your observation point. A covert observation point is more likely to be viewed as physical surveillance;
- C) (U//FOUO) Whether the observation is done from a stationary position or a moving position, and, whether the purpose of moving is limited to obtaining a license plate number or other identifying information. Moving for purposes of following the person to ascertain where he or she is going is more likely to be physical surveillance; and
- D) (U//FOUO) Whether the observation is being done with the unaided eye. Aided observation by telephoto lenses or binoculars, particularly for an extended period, is more likely to be physical surveillance.

(U//FOUO) ***Surveillance Enhancement Devices:*** The use of mechanical devices operated by the user (e.g., binoculars; hand-held cameras; remotely operated, continuously monitored cameras; radiation, chemical or biological detectors) is authorized as part of physical surveillance provided that the device is not used to collect information in which a person has a reasonable expectation of privacy (e.g., equipment such as a parabolic microphone or other listening device that would intercept a private conversation or thermal imaging a home is not permitted). CCTV/Video Surveillance as defined in DIOG Section 18.6.3.3.A is not authorized for use during an Assessment (e.g., a pole camera cannot be used during an Assessment if it is not continuously monitored, even if it is set to surveil an area in which there is no reasonable expectation of privacy).

18.5.8.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Assessments, Predicated Investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3.

18.5.8.3 (U) APPROVAL

(U//FOUO) During an Assessment, physical surveillance may be approved for a period of time not to exceed 72 hours as explained further below.

18.5.8.3.1 (U//FOUO) STANDARDS FOR OPENING OR APPROVING PHYSICAL SURVEILLANCE DURING AN ASSESSMENT

(U//FOUO) During an Assessment, in addition to the standards contained in DIOG Sections 5.5 and 5.8, the FBI employee and supervisor must consider the following:

- A) (U//FOUO) Whether the physical surveillance is rationally related to the articulated purpose and objective of the Assessment;
- B) (U//FOUO) Whether the physical surveillance is the least intrusive alternative for acquiring needed information;
- C) (U//FOUO) If the physical surveillance is for the purpose of determining a pattern of activity, whether there is a logical nexus between the purpose of the Assessment and the pattern of activity the employee is seeking to determine; and
- D) (U//FOUO) If being conducted in order to gather positive foreign intelligence, whether the surveillance is consistent with the requirement that the FBI employee operate openly and consensually with a USPER, to the extent practicable.

18.5.8.3.2 (U//FOUO) 72-HOUR PERIOD FOR ASSESSMENTS

(U//FOUO) In an Assessment, an FBI employee must use the FD-71 or Guardian (for Type 1 & 2 Assessment activities) or an EC (for Type 3, 4, and 6 Assessment activities) to request SSA or SIA approval prior to conducting physical surveillance. If exigent circumstances arise, the FBI employee can conduct physical surveillance without prior approval but must within 24-hours complete an FD-71, Guardian, or EC seeking supervisor approval for the surveillance.

(U//FOUO) In the appropriate system (FD-71 or Guardian), the reason and objective of the physical surveillance must be documented, and the approved 72-hour period of surveillance must begin as stated in the plan at the opening of surveillance. During the 72-hour period, there is no limitation on the use of continuous fixed or moving physical surveillance so long as the activities are consistent with the reason approved by the SSA or SIA. The SSA or SIA may approve physical surveillance requests in incremental periods no longer than 72-hours each. The employee cannot submit one request for multiple 72-hour periods of physical surveillance to the supervisor. For example, if supervisory approval is acquired for a documented plan which specifies that a surveillance will begin at 8:00 a.m. on Monday, September 15, 2008, the 72-hour period of surveillance will expire at 8:00 a.m. on Thursday, September 18, 2008. At or near the end of a 72-hour period of time, if the employee

determines that additional physical surveillance is required, the employee may request supervisor authorization to conduct subsequent physical surveillance for an additional period of no more than 72 hours each. All supervisory approvals, if required, and the results of physical surveillance must be documented in the appropriate Assessment or Predicated Investigation file after review by the supervisor.

18.5.8.3.3 (U//FOUO) MOBILE SURVEILLANCE TEAM (MST) OR MOBILE SURVEILLANCE TEAM – ARMED (MST-A)

(U//FOUO) An employee may request the use of an MST or MST-A during an Assessment or Predicated Investigation by documenting the purpose and objective in an FD-71, Guardian, an EC, or other appropriate form requesting Assistant Special Agent in Charge (ASAC) approval.

(U//FOUO) MSTs and MST-As are overseen and managed by the Mobile Surveillance Unit (MSU) at FHIHQ. For additional information on MST resources refer to the CIRG PG.

18.5.8.3.4 (U) AVIATION RESOURCES

(U//FOUO) An FBI employee may request the use of aviation resources, to include Forward-looking Infrared (FLIR) devices mounted in fixed-wing and rotary-wing aircraft, during an Assessment or Predicated Investigation by documenting the reason and objective in an FD-71, Guardian, an EC, or other appropriate form requesting ASAC approval.

18.5.8.3.4.1 (U//FOUO) FORWARD-LOOKING INFRARED (FLIR) CAMERAS

(U//FOUO) Thermal imaging, sometimes called FLIR, cameras may be operated as hand-held devices or mounted in fixed- and rotary-wing aircraft. Infrared cameras produce images of invisible infrared or "heat" radiation. FLIR is used to assist in visual surveillance during various operational scenarios, including perimeter surveillance, search and rescue operations, vehicle pursuits, and to locate fugitives or otherwise to track objects or subjects in open areas or within the curtilage of a dwelling that cannot easily be observed on the ground without detection.

18.5.8.3.4.1.1 (U//FOUO) AIRCRAFT-MOUNTED VIDEO OR FLIR

(U//FOUO) Typically, aerial FLIR is deployed to supplement ground-based physical surveillance to enhance the safety of the mission or when surveillance teams are unable to maintain close-in surveillance because of the risk of detection. The use of thermal imaging, especially during nighttime hours, can alert officers to potential dangers, such as an ambush or suspects hiding in bushes or other perimeter areas. If FLIR is being used for surveillance outside of the home—in open fields, forests, highways, and possibly, the area surrounding a home, known as the curtilage—a search warrant is not required because those areas do not enjoy Fourth Amendment protection from aircraft-mounted surveillance. If FLIR is being used to obtain information regarding the interior of the home that is otherwise unknowable without physical intrusion, it likely constitutes a search subject to the requirements of the Fourth Amendment.

(U//FOUO) *Example of a use of FLIR that requires a search warrant:* if used to detect heat emanating from within a home to make inferences about the use of high-powered marijuana-growing lamps inside the home (Kyllo v. United States, 533 U.S. 27 (2001)).

(U//FOUO) If a aircraft-mounted FLIR device is to be used:

- 1) (U//FOUO) The aircraft must be in public airspace and comply with Federal Aviation Administration (FAA) regulations regarding altitude;
- 2) (U//FOUO) Overflights of private residential neighborhoods should be avoided if operationally feasible;
- 3) (U//FOUO) To the extent heat signatures may be incidentally collected from homes (not the curtilage), no affirmative investigative use may be made of such information, unless exigent circumstances or other authorization permits its use; and
- 4) (U//FOUO) FLIR surveillance designed to capture and qualitatively analyze the heat signature of a private residence cannot be authorized without a properly issued search warrant (or applicable exception).

(U//FOUO) CDC review must be obtained for aircraft-mounted FLIR when the use exceeds the specific DIOG restrictions as set forth in Section 18.5.8.2.4.1.1.2 above. In such investigations, CDC review is needed to determine whether additional legal requirements apply to the use of aircraft-mounted FLIR equipment (i.e., a court order). Such additional review must be documented in an EC requesting approval for the exceptional use of aircraft-mounted FLIR; such use may not be authorized in an Assessment.

18.5.8.3.4.2 (U//FOUO) AVIATION VIDEO SURVEILLANCE

(U//FOUO) The following guidelines govern the use of video equipment that is permanently mounted to an aircraft and to the operation of FLIR equipment when there is no intrusion into areas in which a person has a reasonable expectation of privacy. Such recordings must be maintained in the investigative electronic surveillance (ELSUR) subfile. The following procedures must be followed:

- A) (U//FOUO) Each flight must use new recording media. The recording must begin when the sensor is deployed, it may not be stopped and restarted, and the entire investigative mission must be recorded;
- B) (U//FOUO) Each recording media must be labeled with the following information: FBI file number, date, operator name and initials, time on and time off; and
- C) (U//FOUO) Each recording media must be treated as an original. For those aircraft that have the capability to create two recordings simultaneously, both must be treated as originals.

18.5.8.3.4.3 (U//FOUO) COMPLIANCE AND MONITORING

(U//FOUO) Authorization documents regarding the use of FLIR and aviation video surveillance must be documented in the investigative ELSUR file.

18.5.8.4 (U) OTHER PHYSICAL SURVEILLANCE

(U//FOUO) Physical surveillance conducted by employees, other than through use of the resources discussed above (i.e., MSTs, MST-As and aviation), during a Predicated Investigation does not require supervisory approval. In addition, the 72 hour time limitation on the use of MST or MST-A is not applicable during Predicated Investigations.

18.5.8.5 (U) MAINTAIN A "SURVEILLANCE LOG" DURING PHYSICAL SURVEILLANCE

(U//FOUO) A surveillance log must generally be maintained for the purpose of documenting observations made during the period of physical surveillance. The log is a chronological narrative detailing the observations noted during the surveillance. A team member must be assigned to maintaining the surveillance log. At the end of the shift, each individual must initial on the surveillance log the notations of the activities he or she observed. Completed surveillance logs must be incorporated into the investigative file. Any original notes must be permanently retained in a 1A envelope (FD-340a) in the investigative file. Surveillance logs must be concise and factual. When reporting locations, the surveillance log must be as specific as possible. Surveillance team members must avoid over-reporting and including unnecessary information; logs are subject to discovery in legal proceedings.

18.5.8.6 (U) USE/DISSEMINATION

(U//FOUO) The use or dissemination of information obtained by this method must comply with the AGG-Dom and DIOG Section 14.

This Page is Intentionally Blank.

18.5.9 (U) INVESTIGATIVE METHOD: GRAND JURY SUBPOENAS – FOR TELEPHONE OR ELECTRONIC MAIL SUBSCRIBER INFORMATION ONLY (IN TYPE 1 & 2 ASSESSMENTS)

(U) See AGC-Dom, Part II.A.4.i.

(U) See DIOG Section 18.6.5 for additional information on use of Federal Grand Jury (FGJ) subpoenas in Predicated Investigations.

18.5.9.1 (U) SCOPE

(U//FOUO) During a Type 1 & 2 Assessment, an FBI employee may request from an appropriate USAO the issuance of a FGJ subpoena for the limited purpose of obtaining subscriber information associated with a telephone number or e-mail address. A FGJ subpoena, under this provision, may not be requested for the purpose of collecting foreign intelligence. For more information regarding FGJ subpoenas, see DIOG Section 18.6.5.

18.5.9.2 (U) APPLICATION

(U//FOUO) This investigative method may be used only in Type 1 & 2 Assessments. It may not be used in a Type 3, 4, 5, or 6 Assessment.

18.5.9.3 (U) APPROVAL

(U//FOUO) In Type 1 & 2 Assessments, telephone and electronic mail subscriber information may be requested through the use of an FGJ subpoena without supervisory approval. An agent requesting a grand jury subpoena during an Assessment must advise the AUSA, who will issue the subpoena, that the FBI is conducting an Assessment. The AUSA must determine whether there is sufficient connection between the Assessment and possible criminal conduct to warrant issuance of a FGJ subpoena. FGJ subpoenas may not be sought during a Type 3, 4, 5, or 6 Assessment.

18.5.9.4 (U) ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) (18 U.S.C. §§ 2701-2712)

(U//FOUO) 18 U.S.C. § 2703(c)(2) states that “a provider of electronic communication service or remote computing service shall disclose to a governmental entity the: (i) name; (ii) address; (iii) local and long distance telephone connection records, or records of sessions, times and durations; (iv) length of service (including start date) and types of service utilized; (v) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (vi) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses a Federal Grand Jury subpoena.” However, in Type 1 & 2 Assessments only subscriber information may be obtained through the issuance of a FGJ subpoena, other customer information described above can only be obtained in a Predicated Investigation. See DIOG Sections 18.6.4 – 18.6.8.

18.5.9.5 (U) USE/DISSEMINATION

(U//FOUO) Because judicial districts vary as to whether subscriber records obtained through use of a FGJ subpoena must be handled pursuant to the FGJ secrecy rules as “matters before the grand jury,” subscriber records obtained pursuant to a FGJ subpoena should be protected as required by the judicial district (e.g., USAO) in which the FGJ subpoena is issued. In addition, in those judicial districts in which subscriber records obtained pursuant to a FGJ subpoena are considered to be “matters before the grand jury,” no documentation of the actual subscriber records should be made in the FD-71 or Guardian. Instead, a copy of the FGJ subpoena and the responsive subscriber records must be filed in a 1A, 1B, or 1C and uploaded to the GJ subfile. Due to developing law on this issue, employees should consult with the AUSA to determine whether such documents are considered to be FGJ materials and must handle them accordingly. The use or dissemination of information obtained by this method must comply with the AGG-Dom, DIOG Section 14, and the Federal Rules of Criminal Procedure (FRPC) Rule 6.

18.6 (U) AUTHORIZED INVESTIGATIVE METHODS IN PRELIMINARY INVESTIGATIONS

(U) See AGG-Dom, Part II.B and Part V.A.1-10.

(U) In Preliminary Investigations the authorized methods include the following:

A) (U) The investigative methods authorized for Assessments:

- 1) (U) Public information. (See Section 18.5.1)
- 2) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
- 3) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
- 4) (U) On-line services and resources. (See Section 18.5.4)
- 5) (U) CHS use and recruitment. (See Section 18.5.5)
- 6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
- 7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
- 8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)

B) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)

C) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)

D) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)

E) (U) Administrative subpoenas. (See Section 18.6.4)

F) (U) Grand jury subpoenas. (See Section 18.6.5)

G) (U) National Security Letters. (See Section 18.6.6)

H) (U) FISA Order for business records. (See Section 18.6.7)

I) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)¹⁶

J) (U) Pen registers and trap/trace devices. (See Section 18.6.9)

K) (U) Mail covers. (See Section 18.6.10)

L) (U) Polygraph examinations. (See Section 18.6.11)

M) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)

N) (U) Undercover operations. (See Section 18.6.13)

¹⁶ (U//FOUO) The use of Search Warrants to obtain this information in Preliminary Investigations is prohibited. (See DIOG Section 18.6.8.4.2.3)

This Page is Intentionally Blank.

18.6.1 (U) INVESTIGATIVE METHOD: CONSENSUAL MONITORING OF COMMUNICATIONS, INCLUDING ELECTRONIC COMMUNICATIONS

18.6.1.1 (U) SUMMARY

(U) Monitoring of wire, oral or electronic communications based on the consent of one party to the communication is referred to as consensual monitoring. The consent exception applies to the interception of wire, oral, and electronic communications. Consensual monitoring requires review by the CDC (Office of Origin – Field Office) or the OGC (Office of Origin – FBIHQ). (AGG-Dom, Part V.A.4)

18.6.1.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Predicated Investigations, positive foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3 or law. This method cannot be used during an Assessment.

(U//FOUO) For those state, local and tribal governments that require all-party consent and do not sanction or provide a law enforcement exception for one-party consent recording of communications with persons within their jurisdiction, OIA approval by an SAC is required. This approval authority is delegable to an ASAC or SSA. The SAC of the employee who is seeking to conduct the consensual monitoring is the approving official for this OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.

(U//FOUO) The law of the state or territory where the consenting party is located when making the recording will govern whether OIA approval is needed.

(U//FOUO) See the OGC website for a list of all-party consent states. See also DIOG Section 18.6.1.6, below.

18.6.1.3 (U) LEGAL AUTHORITY

- A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;
- B) (U) The Wiretap Statute, 18 U.S.C. § 2511-2522, prohibits the intentional interception and use of wire, voice, or electronic communications absent an exception;
- C) (U) The consensual monitoring exceptions, 18 U.S.C. § 2511(2)(c) & (d), require one party to the communication to consent to monitoring; and
- D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq. provides that if a party to the communication has consented to monitoring, a FISA court order is not required.

18.6.1.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is based on the consent of a party to the

communication. Two other statutory exceptions to the general prohibition include 1) the warrant or court order exception, and 2) the computer trespasser exception. This section discusses the monitoring of communications under the consent exception.

(U) Consensual monitoring is the monitoring of communications based on the consent of a party to the communication. (AGG-Dom, Part VII.A.) For purposes of this policy, at least one of the parties to the communication must be located, or the interception of the consensual communication must occur, within the United States or the United States territories. The consensual monitoring of communications is subject to legal review by the CDC or OGC, as applicable. (AGG-Dom, Part V.A.4). Consensual monitoring includes the interception of the content of communications and typically falls into one of three general categories:

- A) (U) Wire communications, which include conventional telephone communications or other means of transmitting the human voice through cable, wire, radio frequency (RF), voice over Internet Protocol (VoIP), or other similar connections;
- B) (U) Oral communications, typically intercepted through the use of devices that monitor and record oral conversations (e.g., a body transmitter or recorder or a fixed location transmitter or recorder used during face-to-face communications in which a person would have a reasonable expectation of privacy but for the consent of the other party); and
- C) (U) Electronic communications, which include any transfer of signs, signals, writing, images, sounds, data, or intelligence by a wire, radio, electronic, or optical system or network (e.g., e-mail, instant message, chat sessions, text messaging, non-voice peer-to-peer communications), as that term is defined in 18 U.S.C. § 2510(12)(14) and (17), which are intercepted and recorded at the time of transmission. The monitoring of electronic communications based on one party consent is sometimes referred to as "consensual computer monitoring." "Consensual computer monitoring" applies to "real time" electronic surveillance based on consent and does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

(U) Note regarding electronic communications monitoring: Agents seeking to consensually monitor electronic communications (specifically, communications to, through, or from a computer) must consider whether the party who has consented is a party to all of the communications they want to monitor or whether some of the communications involve a computer trespasser, as defined by the computer trespasser exception. (See DIOG Section 18.6.2) The trespasser exception and the consensual monitoring of communications exceptions are related, but separate, exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer or computer network can consent to the monitoring of only those communications they send or receive (i.e., to which they are a party), which typically does not include a trespasser's communications. The trespasser exception allows the interception of the communications transmitted to or from the trespasser.

(U) When applicable, the exceptions to the Wiretap Statute can be used together, permitting the interception of the communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, use of both the

consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications.

18.6.1.5 (U) STANDARDS AND APPROVAL REQUIREMENTS FOR CONSENSUAL MONITORING

18.6.1.5.1 (U) GENERAL APPROVAL REQUIREMENTS

(U//FOUO) Except as provided below, an SSA may approve the consensual monitoring of communications if the information likely to be obtained is relevant to an ongoing Predicated Investigation. SSA approval, documented through the FD-759, is conditioned on the following criteria being met and documented on the FD-759 and other supporting documentation:

18.6.1.5.1.1 (U) REASONS FOR MONITORING

(U//FOUO) The synopsis must include sufficient factual information supporting the need for the monitoring. It must provide the relationship between the monitoring and the investigative purpose (e.g., obtain evidence of drug trafficking, public corruption, etc.).

18.6.1.5.1.2 (U) DOCUMENTED CONSENT OF A PARTY TO THE COMMUNICATION TO BE MONITORED

(U//FOUO) Consent must be obtained from one of the parties to be monitored, and the consent must be documented to the investigative ELSUR subfile. Having the consent of one of the parties provides an exception to the Title III statute. The requirement to obtain and document consent also applies to the monitoring of computer communications. See DIOG Section 18.6.1.7.1.1 for specific procedures.

18.6.1.5.1.3 (U) SUBJECT

(U//FOUO) Agents conducting consensual monitoring must not intentionally intercept third-parties who are not of interest to the investigation except for unavoidable or inadvertent overhears.

18.6.1.5.1.4 (U) LOCATION OF DEVICE

(U//FOUO) Consensual monitoring can only be approved if appropriate safeguards are in place to ensure that the consenting party remains a party to the communication throughout the course of monitoring. For example, if a fixed-location monitoring device is being used, the consenting party must be admonished and agree to be present during the duration of the monitoring. If practicable, technical means must be used to activate monitoring only when the consenting party is present.

18.6.1.5.1.5 (U) NOTICE OF CONSENSUAL MONITORING TO OTHER FIELD OFFICES

(U//FOUO) If an employee, CHS, or non-confidential third party is operationally tasked to conduct consensual monitoring outside the field office's territory, the FBI employee requesting approval to conduct the monitoring must provide notice to the SSA who is

responsible for the investigative program in the field office where the monitoring will occur. This notice must be documented in the appropriate investigative file. If the actual monitoring is conducted at a remote recording facility, no notice is required to be given to the field office where the remote recording facility is located.

(U//FOUO) *For example:* A CHS from New Haven is tasked to travel to New York City for a meeting that will be consensually recorded. The New Haven FBI employee must notify the appropriate New York SSA of the consensual monitoring, which will take place in NY. If the CHS is tasked to travel to New York where he/she opens a consensually monitored telephone call using a remote recording facility to monitor the call (and the remote recording facility is in Richmond) notice must be provided to the appropriate SSA in New York, but notice is not required to be given to Richmond.

18.6.1.5.1.6 (U) DURATION OF APPROVAL

(U//FOUO) The request for approval must state the length of time needed for monitoring. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances. If one or more sensitive monitoring circumstances is present, DOJ may limit its approval to a shorter duration. See DIOG Section 18.6.1.6.3 below.

18.6.1.5.1.7 (U) LEGAL REVIEW

(U//FOUO) Prior to the opening of consensual monitoring, the CDC or OGC must concur that, given the facts of the investigation, the consensual monitoring is legal. Although AUSA concurrence is no longer required for consensual monitoring, providing notice to the AUSA is encouraged.

18.6.1.5.1.8 (U) CHANGE OF MONITORING CIRCUMSTANCES

(U//FOUO) Whenever the monitoring circumstances change substantially, a new FD-759 must be executed, and the CDC or OGC must be recontacted to obtain new concurrence. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in monitoring circumstances which require a new FD-759: a different consenting party, a change in the location of a fixed monitoring device, or the addition of a new computer system. If any of these or other monitoring circumstances substantially change, the FBI employee must immediately contact the CDC or OGC.

18.6.1.5.1.9 (U) JOINT INVESTIGATIONS

(U//FOUO) In joint investigations, the policy and procedures for conducting any investigative method or investigative activity by employees or CHSs are usually governed by FBI policy. Similarly, employees from other agencies who are participating in a joint investigation with the FBI are generally governed by their agencies' policies regarding approvals. If, however, the FBI has assumed supervision and oversight of another agency's employee (e.g., a full time JTTF Task Force Officer), then FBI policy regarding investigative methods or investigative activity controls. Similarly, if another agency has assumed supervision and oversight of a FBI employee, unless otherwise

delineated by MOU, the other agency's policy regarding investigative methods or investigative activity controls.

(U//FOUO) Consensual monitoring conducted by a non-confidential party (e.g., witness, victim, etc.) will be controlled by the agency that is primarily responsible for the non-confidential party. In a joint investigation, the employees should reach an understanding as to which agency is responsible for the non-confidential party; that agency's policies will govern approval and documentation requirements for consensual monitoring.

18.6.1.6 (U) CONSENSUAL MONITORING SITUATIONS REQUIRING ADDITIONAL APPROVAL

18.6.1.6.1 (U) PARTY LOCATED OUTSIDE THE UNITED STATES

(U//FOUO) Some countries are known to prohibit one-party consensual recording of persons within their country. An employee who is seeking to consensually monitor a person known to be located in such a country must submit an FD-759 with a cover EC to the appropriate FBIHQ Section Chief who is responsible for the investigative program for approval. Such a request may only be approved following consultation with the DOJ, Criminal Division, Office of International Affairs, and upon a determination by the appropriate FBIHQ Section Chief that the benefit of using the technique outweighs the risks involved. The EC will also include a notification copy to the appropriate IOD Section Chief. The IOD may provide to the responsible Section Chief any information it deems relevant in considering such a request, including its view whether the potential benefit of using the investigative method outweighs the potential diplomatic risks involved. A list of countries to which this policy applies is available in DIOG Appendix G.

(U//FOUO) If a non-consenting party initiates a communication that is known to originate from a country that opposes one-party consents, the communication may be recorded without FBIHQ approval but the IOD must be notified as soon as practicable after the communication has been concluded.

(U//FOUO) When engaged in consensual computer monitoring, the location of the non-consenting party is often unknown and can easily be masked. The notice and approval requirements discussed above do not apply if the location of the party to the communication is not known to be in one of those countries. Nevertheless, if the investigation identifies the country where a non-consenting party is located, and that country is one known to oppose one-party consent and does not have an exception for law enforcement, the above procedures should be followed.

(U//FOUO) If neither party to the communication is located within the United States, the United States territories, or outside the territories of all countries, the DIOG does not govern; rather, the AGG for Extraterritorial FBI Operations and Criminal Investigations control for criminal investigations or the NSIG portions regarding extraterritorial operations control for national security investigations and collection of foreign intelligence. In such investigations, consultation with the appropriate Legat and IOD is required. See DIOG Section 13.

18.6.1.6.2 (U) CONSENT OF MORE THAN ONE PARTY REQUIRED FOR CONSENSUAL MONITORING

(U//FOUO) For those state, local and tribal governments that require all-party consent and do not sanction or provide a law enforcement exception for one-party consent recording of communications with persons within their jurisdiction, otherwise illegal activity (OIA) approval by an SAC is required. This approval authority is delegable to an ASAC or SSA. The SAC of the employee who is seeking to conduct the consensual monitoring is the approving official for this OIA. Prior to the SAC authorizing the OIA, one-party consent must be acquired.

(U//FOUO) The law of the state or territory where the monitoring will take place will govern whether OIA approval is needed.

(U//FOUO) Consensual monitoring authority and OIA in all-party consent states with no law enforcement exception for FBI employees and non-confidential parties may be authorized for the duration of the investigation, unless specified otherwise, and the authorization must be appropriately documented. As noted in DIOG Section 17.4 above, OIA authority for a CHS must be approved in conformity with the AGG-CHS and the FBI CHSPG.

(U//FOUO) **FBI employee and non-confidential party (OIA):** When OIA consensual monitoring will be conducted by an FBI employee or a non-confidential party, the OIA approval must be obtained from the SAC of the employee who is seeking to conduct the consensual monitoring, and the approval must be documented in a properly executed FD-759. This approval authority is delegable to an ASAC or SSA. Such OIA may be granted for the duration of the investigation, as long as the consensual monitoring circumstances do not materially change.

(U//FOUO) **CHS (OIA):** When OIA consensual monitoring will be conducted by a CHS, the OIA approval must be obtained from the SAC of the field office in which the CHS is handled. This approval authority is delegable to an ASAC or SSA. Such OIA approval may be granted for a maximum of 90 days, with no additional OIA documentation required for monitoring during that period. If it is necessary to extend the OIA for consensual monitoring beyond the initial 90 day period, another FD-759 may be used or, alternatively, such OIA for consensual monitoring may be requested, approved, and documented with an EC to the CHS file consistent with the AGG-CHS and the FBI's CHSPG. The original and all subsequent FD-759s used to document the OIA approval for the CHS must be maintained in the CHS file. A copy of the FD-759 must also be filed in the investigative file or any ELSUR subfile as appropriate

(U//FOUO) See the OGC website for a list of all-party consent states. See, also DIOG Section 18.6.2, below.

18.6.1.6.3 (U) SENSITIVE MONITORING CIRCUMSTANCE

(U) Requests to monitor communications when a sensitive monitoring circumstance is involved must be approved by the DOJ Criminal Division, or, if the investigation concerns a threat to the national security or foreign intelligence collection, by the DOJ NSD. (AGG-Dom, Part V.A.4) A "sensitive monitoring circumstance" is defined in the AGG-Dom, Part VII.O, to include the following:

- A) (U) Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years (Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315);
- B) (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- C) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation;
- D) (U) A party to the communication is in the custody of the Bureau of Prisons (BOP) or the United States Marshal Service (USMS) or is being or has been afforded protection in the Witness Security Program. A sensitive monitoring circumstance is not triggered if an FBI employee seeks to record an interview with an individual in the custody of the BOP or the USMS and the FBI employee has identified himself/herself as an FBI employee by clothing, display of credential or badge, or other means. This exception to required DOJ approval does not eliminate the requirement to obtain SAC approval to record such an interview.
- E) (U//FOUO) The use of a prisoner who is in the custody of the BOP or the USMS as the consenting party is a "sensitive monitoring circumstance" that requires additional information before DOJ will approve. Accordingly, field offices are required to coordinate the use of a prisoner, who is the subject of consensual or non-consensual monitoring, through the responsible FBIHQ operational section. If the individual is in the custody of the BOP or the USMS, and the field office wishes to use the prisoner to consensually monitor a conversation, the field office EC requesting approval to use a prisoner in order to consensually monitor communications, or a request for a furlough or extraordinary transfer of a prisoner to make the consensual recording, must contain the following additional information:
 - 1) (U//FOUO) Location of the prisoner;
 - 2) (U//FOUO) Identifying data concerning the prisoner (FBI number, inmate identification number, social security number, etc.);
 - 3) (U//FOUO) Charge for which prisoner is incarcerated, including date of conviction, sentence, Judicial District;
 - 4) (U//FOUO) Prisoner's arrest record and a summary of the investigation, if applicable;
 - 5) (U//FOUO) Necessity for using the prisoner in the investigation;
 - 6) (U//FOUO) The target of the investigation and his or her role in the crime or organization under investigation;
 - 7) (U//FOUO) The prisoner's relationship or association with the target;
 - 8) (U//FOUO) A statement whether the target is aware of the prisoner's cooperation with law enforcement and if so, the cover story that will be used for the prisoner's safety;
 - 9) (U//FOUO) Nature of the activity requested (e.g., wear consensual monitoring device, furlough, extraordinary transfer) and a detailed explanation of the role the prisoner is to perform;
 - 10) (U//FOUO) Security measures that will be taken to ensure the prisoner's safety, if necessary, alleviate risk to the public, and to prevent the prisoner's escape;
 - 11) (U//FOUO) Length of time the prisoner will be needed in the activity;

- 12) (U//FOUO) Whether the prisoner will be needed as a witness;
- 13) (U//FOUO) Whether a prison redesignation (relocation) will be necessary upon completion of the activity;
- 14) (U//FOUO) Whether the prisoner will remain in the custody of the FBI, be housed in jails or similar facilities at certain times, and whether he/she will be unguarded except for security purposes;
- 15) (U//FOUO) Number of officers on the security detail;
- 16) (U//FOUO) Name, address, and telephone number of the federal prosecutor endorsing the request and a statement from the prosecutor regarding entrapment; and
- 17) (U//FOUO) Statement whether the FBI, USMS, or BOP has knowledge or information whether the prisoner has an attorney and, if so, whether the attorney has concurred with his or her client's use.

(U//FOUO) If approval is obtained, the field office must also:

- A) (U//FOUO) Submit an interim progress report if a continuance beyond the date originally projected for conclusion is needed. A detailed report must be submitted at the conclusion of activity; and
- B) (U//FOUO) If the prisoner is unsentenced or on writ status, a sealed court order must be obtained after the request has been approved.
- C) (U//FOUO) See the classified provisions in DIOG Appendix G for additional information regarding consensual monitoring.

(U//FOUO) **Procedure for Obtaining DOJ Approval For a Sensitive Monitoring Circumstance:** In order to obtain DOJ approval for consensual monitoring when a sensitive monitoring circumstance is involved, the field office must execute an FD-759 and also prepare a cover EC and letterhead memorandum (LHM) for dissemination by FBIHQ to DOJ. The LHM must reiterate the information contained in the executed FD-759 and must be reviewed and approved by the CDC or OGC prior to submission to DOJ.

(U//FOUO) **Emergency requests involving Sensitive Monitoring Circumstances:** Oral approval from DOJ can be obtained for exigent requests for consensual monitoring involving "sensitive monitoring circumstances" (e.g., when the communication to be monitored is expected to take place before written approval from DOJ can, with due diligence, be obtained) by calling:

- A) (U//FOUO) **For Criminal matters:** The Director or an Associate Director of the Criminal Division's Office of Enforcement Operations, or the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division at (202) 514-6809; in the normal course, the field office should contact the OEO duty attorney with the request for emergency approval at (202) 514-5000; or
- B) (U//FOUO) **For National Security matters:** The Office of Intelligence, NSD or the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for National Security at (202) 514-5600.

(U//FOUO) **Note:** After normal duty hours, the DOJ command center at (202) 514-5000 can provide a contact number for either the Criminal Division or NSD duty attorney.

(U//FOUO) Such oral approval must be reduced to writing and submitted to the appropriate FBIHQ official as soon as practicable but within five business days after authorization has been obtained.

(U//FOUO) If an emergency situation requires monitoring at a time when none of the individuals identified above can be reached, emergency approval may be given by the SAC with notice to FBIHQ operational section and the appropriate DOJ division as soon as practicable after the emergency monitoring is authorized, but in all events within five business days of the emergency authorization. Emergency authority granted by the SAC (or, as delegated, by the ASAC) cannot exceed 30 days and requests for extension must be submitted to FBIHQ for DOJ approval.

18.6.1.7 (U) DURATION OF APPROVAL

(U//FOUO) Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances. If one or more sensitive monitoring circumstances is present, DOJ may limit its approval to a shorter duration.

18.6.1.8 (U) SPECIFIC PROCEDURES

(U//FOUO) The following procedures apply when obtaining consent.

18.6.1.8.1 (U) DOCUMENTING CONSENT TO MONITOR/RECORD

(U//FOUO) Whenever possible, written consent must be obtained from the consenting party. Written consent must be documented on an FD-472 (Consent to Record), an FD-1071 (Consent to Monitor Content of Electronic Communications), or any subsequent form as appropriate. If the consenting party is an FBI employee or a law enforcement or intelligence officer, a properly executed and properly witnessed consent form must be obtained and maintained in the appropriate ELSUR sub-file. For CHSs, this documentation must be maintained in the CHS file. If a copy of the consent form is placed in an investigative or ELSUR subfile, it must not contain the true name of the CHS. The CHS's symbol number or alias name should be used.

(U//FOUO) If the consenting party is not a CHS, FBI employee, or other law enforcement or intelligence officer (i.e., a "non-confidential party"), and declines to provide a written consent, oral consent is acceptable. When oral consent is obtained, at least two law enforcement or intelligence officers (one of whom must be a FBI agent or a deputized TFO) must witness the consent, and the consent must be memorialized in an FD-302. The fact that the consenting party has declined to give written consent should also be recorded on the FD-472 (Consent to Record) or FD-1071 (Consent to Monitor Content of Electronic Communications), or subsequent form as appropriate. This form must be completed by the agent or TFO with the exception of the consenting party's signature. The consent forms remain valid until such time as the consenting or authorizing party revokes the consent or authorization, either orally or in writing, to an agent of the FBI or FBI Task Force Officer. The consent form must be maintained in the appropriate ELSUR subfile.

18.6.1.8.1.1 (U) CONSENSUAL MONITORING OF COMPUTERS

(U//FOUO) When relying on the consent exception to monitor computer communications and the computer or other communication device to be monitored is known to be used by more than one person, the consent of each and every person whose communications are to be monitored must be documented. When documents or other circumstances (e.g., an employee agreement, a terms of use document, a corporate or organizational consent form) are relied upon to establish implied consent, a complete description of the relevant circumstances, including a copy of any language or document establishing implied consent, must be documented to the file via EC. Before the monitoring is approved or initiated, the CDC or OGC must review the document at issue to ensure that the implied consent is legally sufficient.

18.6.1.8.2 (U) DOCUMENTING APPROVAL

(U//FOUO) The case agent must document the approval by filing an executed and approved FD-759 in the ELSUR subfile.

18.6.1.8.3 (U) RETENTION OF CONSENSUALLY MONITORED COMMUNICATIONS

(U//FOUO) The case agent must maintain and store the original recording pursuant to applicable ELSUR program policy (See ELSUR Guide, Electronic Surveillance Manual, and Electronic Surveillance Issues located in the OGC Main Law Library).

18.6.1.8.4 (U) MULTIPLE COMMUNICATIONS

(U//FOUO) In investigations in which various modes of communication may be consensually monitored (e.g., telephonic, non-telephonic, electronic communications, etc.), one FD-759 may be used to document approval, provided that each mode of communication to be monitored is being used in the same investigative file and all facts required on the FD-759 are the same. If the material facts on the FD-759 vary (e.g., more than one consenting party, different periods of authority, etc), separate FD-759s must be executed and included in the ELSUR subfile.

18.6.1.8.5 (U) INVESTIGATION SPECIFIC APPROVAL

(U//FOUO) Approval for consensual monitoring of communications is investigation specific and is not transferable to any other investigation, unless the investigative file under which the authority was granted is consolidated or reclassified. Additional approval must be obtained for any spin-off investigation(s) that arises out of the original investigation.

18.6.1.9 (U) COMPLIANCE AND MONITORING

(U//FOUO) Case agents and supervisors must regularly monitor the use of this method to ensure that the continued interception of communications is warranted and lawfully obtained by virtue of consent, express or implied, from a party to the communication. Such monitoring shall include a review of the investigative file to ensure that consent and authorization forms are in the ELSUR subfile and properly completed by the requesting agent. ELSUR program personnel must review all submitted FD-759s and consent forms (FD-472 and FD-1071) to ensure proper approval is documented for the consensual monitoring of communications.

18.6.2 (U) INVESTIGATIVE METHOD: INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

18.6.2.1 (U) SUMMARY

(U) The wire or electronic communications of a computer trespasser to, from, or through a protected computer may be intercepted and collected during a Predicated Investigation. Use of this method requires SSA approval and review by the CDC (Office of Origin – Field Office) or the OGC (Office of Origin – FBIHQ). (AGG-Dom, Part V.A.4)

18.6.2.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Predicated Investigations, positive foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. This method cannot be used during an Assessment.

18.6.2.3 (U) LEGAL AUTHORITY

- A) (U) The Fourth Amendment to the United States Constitution and case law interpreting the same;
- B) (U) The Wiretap Statute, 18 U.S.C. § 2511, prohibits the intentional interception and use of wire, oral, or electronic communications absent an exception;
- C) (U) Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i); and
- D) (U) The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801 et seq., requires court authorization for “electronic surveillance.” FISA specifically provides, however, that the acquisition of computer trespasser communications that would be permissible under 18 U.S.C. § 2511(2)(i) are not subject to the FISA court order requirement for electronic surveillance of wire communication under section 101(f)(2) of FISA. 50 U.S.C. § 1801(f)(2).

18.6.2.4 (U) DEFINITION OF THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U) Generally, the Wiretap Statute (also referred to as Title III), 18 U.S.C. §§ 2510-2522, prohibits the intentional interception of wire, oral, or electronic communications unless one of several exceptions applies. One such exception is the interception of a computer trespasser's wire or electronic communications to, through or from a protected computer based on the authorization of the owner or operator of that computer. Another statutory exception is based on the consent of a party to the communication. This section relates specifically to the computer trespasser exception; the policy on consensual recording of computer communications can be found at DIOG Section 18.6.1.

(U) The computer trespasser exception to the Wiretap Statute, 18 U.S.C. § 2511(2)(i), permits a person acting under color of law to intercept the wire or electronic communications of a computer trespasser that are transmitted to, through, or from a protected computer when the owner or operator of that computer authorizes the interception. The use of this method does not include retrieving or obtaining records of communications that have been stored on the computer or elsewhere after the communication has occurred.

(U) The statute requires:

- A) (U) The owner or operator of the protected computer to authorize the interception of the trespasser's communications on the protected computer;
- B) (U) The person acting under color of law to be engaged in a lawful investigation;
- C) (U) The person acting under color of law to have reasonable grounds to believe that the contents of the trespasser's communications will be relevant to the investigation; and
- D) (U) The interception is limited to the communications transmitted to or from the trespasser.

(U) The case agent is responsible for documenting the basis for the conclusion that the person who provided authorization to intercept the trespasser's communications is either the owner or operator of the protected computer. The "owner or operator" must have sufficient authority over the protected computer/computer network system to authorize access across the entire system. This could be a corporate officer, CIO, or system administrator, if the system administrator has authority across the entire system. In any instance in which the identification of the owner or operator is not plainly evident, the case agent must seek the assistance of the CDC or the OGC to identify the proper owner or operator.

(U) A "protected computer," defined in 18 U.S.C. § 1030(e), has been generally interpreted to be any computer or computer network device connected to the Internet, although it also includes most computers used by a financial institution or the United States Government regardless of whether the computer is connected to the Internet.

(U) A "computer trespasser" is a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, from, or through the protected computer. The definition of computer trespasser does not include a person known by the owner or operator to have exceeded their authority or to have an existing contractual relationship with the owner or operator for access to all or part of the computer. (18 U.S.C. § 2510(21))

(U) The trespasser exception and the consensual monitoring of communications exception are related, but separate, exceptions to the Wiretap Statute. The owner, operator, and authorized users of a protected computer can consent to the monitoring of only those communications they send or receive (i.e., communications to which they are a party), which do not include a trespasser's communications. (See DIOG Section 18.6.1) In comparison, under the trespasser exception, the owner or operator may only authorize the interception of the communications of a trespasser transmitted to, through or from the protected computer.

(U) When applicable, the computer trespasser and consensual monitoring of communications exceptions to the Wiretap Statute can be used together, permitting the interception of communications of both authorized users and trespassers on the protected computer. This is particularly useful when it is difficult to discern the trespasser communications from other communications. If it is possible to obtain consent to monitor the communications of the authorized users, using the consent and trespasser exceptions together can mitigate the risk of over or under collection of the trespasser's communications. See DIOG Section 18.6.1 for the policy regarding consensual monitoring of computer communications.

18.6.2.5 (U//FOUO) USE AND APPROVAL REQUIREMENTS FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER**18.6.2.5.1 (U) GENERAL APPROVAL REQUIREMENTS**

(U//FOUO) An SSA may approve the use of the computer trespasser exception, subject to CDC or OGC review. Approval is conditioned on the following criteria being met and documented on the FD-759 and through other supporting documentation in the investigative file:

18.6.2.5.1.1 (U) REASONS FOR THE INTERCEPTION

(U//FOUO) The synopsis portion of the FD-759 must include sufficient facts to support the need for the interception and to explain how the contents of the trespasser's communications will be relevant to the investigative purpose.

18.6.2.5.1.2 (U) OWNER OR OPERATOR AUTHORIZATION

(U//FOUO) The authorization of the owner or operator of the protected computer (who may be the system administrator, as stated above) to a person acting under color of law to intercept the trespasser communications on the protected computer system or network must be documented using the FD-1070, Authorization to Intercept the Communications of a Computer Trespasser. The steps the case agent takes to ensure that the person providing the authorization is the actual or appropriate owner or operator of the protected computer must be documented in the investigative file. See 18.6.2.6 below for specific procedures.

18.6.2.5.1.3 (U) ACQUIRING ONLY TRESPASSER COMMUNICATIONS

(U//FOUO) When intercepting communications under the computer trespasser exception alone (i.e., not in conjunction with consensual monitoring of electronic communications), the collection must not intentionally acquire communications other than those to or from the trespasser. This can often be technically complicated to accomplish depending on the use and configuration of the protected computer and the sophistication of the trespasser. The steps to be taken to identify trespasser communications and to isolate such communications from those of authorized users must be considered by the approving and reviewing officials and documented in the investigative file. See DIOG Section 18.6.2.6 below for specific procedures.

18.6.2.5.1.4 (U) OWNER OR OPERATOR COLLECTION

(U//FOUO) The interception of trespasser communications may be conducted by the FBI or by the owner or operator of the protected computer at the FBI's request. In either instance, the interception is being conducted under color of law. If the collection is not being conducted by the FBI, the case agent must document that he or she has informed the person conducting the interception that it must be accomplished in conformity with the statute.

18.6.2.5.1.5 (U) LOCATION OF INTERCEPT

(U//FOUO) If the intercept or collection of the trespasser communications will occur outside of the field office of the approving official, the SAC or ASAC of the field office within which the interception will occur must be notified, and the notification must be documented in the investigative file.

18.6.2.5.1.6 (U) DURATION

(U//FOUO) The request for approval (FD-759) must state the length of time needed for the interception. Unless otherwise warranted, approval may be granted for the duration of the investigation, subject to a substantial change of circumstances, as described in DIOG Section 18.6.2.6, below.

18.6.2.5.1.7 (U) LEGAL REVIEW

(U//FOUO) Prior to the opening of the interception, the CDC or OGC must concur that, given the facts of the investigation, the interception appears to be lawful under the computer trespasser exception. Whenever the factors surrounding the use of the approved technique change substantially, a new FD-759 must be executed. The newly executed FD-759 must include refreshed concurrence of the CDC or OGC. (AGG-Dom, Part V.A.4.) The following are examples of substantial changes in the circumstances of the interception that require a new FD-759: a change in owner or operator, a change in the method of collection, or the change or addition of a protected computer system. On the other hand, technical changes in the collection system for the purpose of improving or refining the interception are usually not substantial changes to the circumstances of the interception.

18.6.2.5.1.8 (U) JOINT INVESTIGATIONS

(U//FOUO) In joint investigations, if the FBI is the lead investigating agency, FBI policies and guidance regarding the interception of computer trespasser communications must be followed. If the FBI is not the lead investigating agency, the policies of the lead investigating agency must be followed and documented to the appropriate FBI investigative file.

18.6.2.5.1.9 (U) EXTRATERRITORIAL CONSIDERATIONS

(U//FOUO) If the investigation involves a computer trespasser or other subjects that the FBI reasonably believes are located in a foreign country, the case agent should consult the DOJ Extraterritorial Guidelines, memoranda of understanding, and FBI guidance regarding proper notification and coordination requirements.

18.6.2.6 (U) DURATION OF APPROVAL FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//FOUO) The interception and collection of computer trespasser communications under the computer trespasser exception may be approved for a specified length of time or for the duration of the particular investigation.

18.6.2.7 (U) SPECIFIC PROCEDURES FOR INTERCEPTING THE COMMUNICATIONS OF A COMPUTER TRESPASSER

(U//FOUO) The following procedures apply when obtaining authorization.

18.6.2.7.1 (U) DOCUMENTING AUTHORIZATION TO INTERCEPT

(U//FOUO) Whenever possible, written authorization must be obtained from the owner or operator of the protected computer and documented on an FD-1070, Authorization to Intercept the Communications of a Computer Trespasser.

(U//FOUO) If the authorization from the owner or operator is provided orally, at least one FBI agent and another law enforcement or intelligence officer should witness the authorization, and the authorization must be memorialized in an FD-302. The fact that the authorizing party has declined or was unable to give written authorization must also be recorded on the FD-1070, Authorization to Intercept the Communications of a Computer Trespasser form. This form should then be executed in all respects with the exception of the authorizing party's signature.

(U//FOUO) The case agent must document to the file (i.e., FD-302 or EC) the facts that establish that the person providing the authorization is a proper party to provide authorization for the anticipated interception.

(U//FOUO) If the case agent is seeking approval for the FBI to engage in both consensual monitoring and an interception of the computer trespasser on the same computer system, separate forms -- one providing consent to monitor the communication to which the consenter is a party and one providing the authorization to intercept the trespasser's communications -- must be completed.

18.6.2.7.2 (U) ACQUIRING ONLY THE TRESPASSER COMMUNICATIONS

(U//FOUO) The computer trespasser exception permits the FBI to intercept only trespasser communications. Prior to seeking approval to intercept computer trespasser communications, the case agent must coordinate the use of the method with the Field Office Technical Advisor by submission of an Electronic Technical Request (ETR). On receipt of the ETR, the Technical Advisor must ensure that the technical equipment and expertise necessary to lawfully implement the interception are timely provided following approval to use this investigative method.

(U//FOUO) Many of the technical challenges and risks associated with accurately isolating the trespasser communications can be mitigated by also obtaining consent to monitor the computer or a court order. The possibility of using the authority to intercept trespasser

communications in conjunction with consent should be raised at the time of the ETR submission or as soon thereafter as the case agent determines that the authorized users of the protected computer will consent to FBI monitoring.

(U//FOUO) When intercepting trespasser communications, the case agent must prepare an FD-302 or EC detailing the steps taken to identify trespasser communications and to isolate such communications from those of authorized users. For example: "reviewed system logs provided by the system administrator and identified a trespasser accessing the system at the following dates and times via IP address xxx or port xxx." Additionally, any subsequent review or revision of the steps needed to identify and isolate the trespasser's communications must also be documented to the investigative file by an EC or FD-302, as appropriate.

18.6.2.7.3 (U) REVIEWING THE ACCURACY OF THE INTERCEPTION

(U//FOUO) At the opening of interception and collection of computer trespasser communications, the Technical Advisor or designated technically trained agent (TTA) coordinating the implementation of the interception and collection device shall ensure that appropriate collection parameters are implemented as required by OTD policy and procedures.

(U//FOUO) The case agent shall ensure a timely initial review of the collected information to verify that the interception and collection are limited to communications authorized for interception and collection under the trespass authority or other lawful exception. Following this initial review, the case agent shall ensure that a similar review and evaluation is repeated at appropriate intervals throughout the duration of the interception to ensure that the interception and collection remain within the scope of the trespasser or other lawful exceptions.

(U//FOUO) Any FBI employee who identifies interception and collection of communications that may be outside the scope of the trespasser or other lawful exception shall immediately notify the case agent and the operational SSA of the possible unauthorized interception and collection of communications. Upon the determination that communications have been unlawfully intercepted or collected, the interceptions and collection must be halted immediately. The case agent must consult with a TTA to determine whether collection may be resumed in a manner that assures further unlawful collections will not occur. If the SSA determines that unlawful collection can be reliably prevented, that determination must be documented to the file before lawful interceptions and collection may resume.

(U//FOUO) The content of communications determined to have been unlawfully collected cannot be used in any manner and shall be removed promptly from all FBI systems and destroyed. A memorandum documenting the removal and destruction shall be filed in the main investigation file and ELSUR Sub File.

18.6.2.7.4 (U) REVIEWING THE RELEVANCY OF THE INTERCEPTION

(U//FOUO) The trespasser exception requires the FBI to have a reasonable belief that the contents of the trespasser's communications will be relevant to the investigation. Following opening of the interception and collection of the trespasser communication, the case agent

must ensure that the collected communications are reviewed, at appropriate intervals throughout the duration of the interception, to determine whether the interception is and continues to be relevant to the authorized investigation.

18.6.2.7.5 (U) DURATION OF APPROVAL

(U//FOUO) Authorization to intercept trespasser communications remains valid until such time as the authorizing party, orally or in writing, revokes the authorization or on the termination date of the authorization, whichever comes first.

18.6.2.7.6 (U) ELSUR REQUIREMENTS

(U//FOUO) The information obtained from the collection must be retained in conformity with the ELSUR Policies (See ELSUR Guide, Electronic Surveillance Manual, and Electronic Surveillance Issues located in the OGC Main Law Library) or other applicable policies.

18.6.2.7.7 (U) MULTIPLE COMMUNICATIONS

(U//FOUO) In investigations in which various modes of communication may be intercepted (e.g., telephonic, non-telephonic, electronic communications, etc., or the use of consensual computer monitoring in conjunction with the interception of trespasser communications), one FD-759 may be used to document approval, provided that each mode of communication to be monitored is being used in the same investigative file and all facts required on the FD-759 are the same. If the material facts on the FD-759 vary (e.g., different periods of authority, etc.), separate FD-759s must be executed.

18.6.2.7.8 (U) INVESTIGATION SPECIFIC APPROVAL

(U//FOUO) Approval for intercepting a computer trespasser's communications is investigation specific and is not transferable to any other investigation, unless the investigative file under which the authority was granted is consolidated or reclassified. Investigation specific approval must be obtained for any spin-off investigation(s) that arises out of the original investigation.

18.6.2.8 (U) COMPLIANCE AND MONITORING

(U//FOUO) Case agents must regularly monitor the use of this method to ensure that the continued interception of trespasser communications is warranted and being lawfully conducted. Such monitoring shall include a review of the investigative file to ensure that consent and authorization forms have been properly executed and filed. ELSUR program personnel must review all submitted FD-759s and FD-1070 (Authorization to Intercept the Communications of a Computer Trespasser form) to ensure proper approval has been documented for the interception of computer trespasser communications.

This Page is Intentionally Blank.

18.6.3 (U) INVESTIGATIVE METHOD: CLOSED-CIRCUIT TELEVISION/VIDEO SURVEILLANCE, DIRECTION FINDERS, AND OTHER MONITORING DEVICES

18.6.3.1 (U) SUMMARY

(U//FOUO) During Predicated Investigations, the FBI may use Closed-Circuit Television/Video Surveillance, Direction Finders, Electronic Tracking Devices, Forward-Looking Infrared (FLIR) Cameras (other than aircraft mounted FLIR, see DIOG Section 18.5.8 for those procedures), and other non-communication monitoring devices. These methods usually do not require court orders or warrants unless they involve monitoring an area or place where there is a reasonable expectation of privacy, physical trespass is required to install the device or non-consensual monitoring of communications will occur. Use of these methods requires prior legal review by the CDC or OGC and SSA approval, except as noted below.

18.6.3.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in Predicated Investigations and positive foreign intelligence collection investigations and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. This method cannot be used during an Assessment.

18.6.3.3 (U) LEGAL AUTHORITY

- A) (U) AGG-Dom, Part V
- B) (U) Tracking devices use (18 U.S.C. § 2510(12)(C))
- C) (U) Rule 41 Federal Rules of Criminal Procedure
- D) (U) Fourth Amendment to the United States Constitution

18.6.3.4 (U) DEFINITION OF INVESTIGATIVE METHOD

- A) (U//FOUO) Closed Circuit Television/Video Surveillance (CCTV/Video Surveillance): a fixed-location video camera/device that is typically concealed from view or that is placed on or operated by a consenting party.
- B) (U//FOUO) Electronic Tracking Devices: Direction finders include electronic tracking devices, such as, radio frequency (RF) beacons and transmitters, vehicle locator units, and various devices that use a Global Positioning System (GPS) or other satellite system for monitoring non-communication activity. Electronic tracking devices are specifically excluded from Title III requirements (18 U.S.C. § 2510(12)(C)). In circumstances where a court order is required (pursuant to FRCP Rule 41(e)(2)(C)), a judge or magistrate may authorize the use of an electronic tracking device within the jurisdiction of the court and outside that jurisdiction, if the device is installed in that jurisdiction. (FRCP Rule 41(b)(4); 18 U.S.C. § 3117)

18.6.3.5 (U//FOUO) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U//FOUO) When a video camera is physically operated as a hand-held video and is used in an area in which no one has a reasonable expectation of privacy, its use is equivalent to using a still camera and does not require CDC review or SSA approval.

(U//FOUO) Except for a hand-held video as described above, CDC or OGC review and SSA approval is required for the use of CCTV/Video Surveillance, tracking devices, and other monitoring devices. CDC review and SSA approval must be documented using the FD-759. SSA approval may be granted if the following criteria have been met:

- A) (U//FOUO) Legal review and concurrence from the CDC or OGC that a court order is not required for installation or use of the device because there has been lawful consent, no reasonable expectation of privacy exists, or no physical trespass is necessary to install the device. Whenever circumstances change in either installation or monitoring, a new legal review must be obtained to determine whether a separate authorization is necessary;
- B) (U//FOUO) Use of the method is reasonably likely to achieve investigative objectives;
- C) (U//FOUO) Appropriate safeguards exist to ensure that unauthorized monitoring does not occur. For example, if a fixed-location monitoring device is used based on the consent of a party, the consenting party must be admonished and agree to be present during the duration of the monitoring, and, if practicable, technical means should be used to activate monitoring only when the consenting party is present.

18.6.3.6 (U) DURATION OF APPROVAL

(U//FOUO) Approval for the use of this method may be for the duration of the investigation, except when: (i) a substantial change occurs in the location of the CCTV/Video Surveillance or monitoring device; (ii) a substantial change occurs in the area to be subjected to CCTV/Video Surveillance; or (iii) there is a change in the primary subject of the surveillance. In each of these circumstances, new approval is required. If a court order is required, the court order will specify the duration of authorization.

18.6.3.7 (U) SPECIFIC PROCEDURES

(U//FOUO) To use this method, the case agent must:

- A) (U//FOUO) Submit an FD-759 for CDC or OGC review and SSA approval for video (not hand-held video where there is no reasonable expectation of privacy), tracking devices, and other monitoring devices.
- B) (U//FOUO) Maintain the approved FD-759 in the field office ELSUR Subfile and a copy in the field office CCTV/Video Surveillance control file.
- C) (U//FOUO) If authorization is based upon consent, obtain consent from both the participant in the activity being monitored/viewed and the person having control over the location where the monitoring device will be installed, if they are not the same person. If it is not possible or practical to obtain written consent, oral consent is permitted if witnessed by two law enforcement officers (one of whom must be an agent of the FBI, deputized task force officer, or other federal agent). A consent form (FD-472) should be executed and properly witnessed

in all situations requiring consent for the monitoring/installation, even if the consenting party is a CHS, FBI employee, or any other law enforcement officer.

- D) (U//FOUO) The OTD policy may also require submission of a written request for the use of certain equipment and personnel.

18.6.3.8 (U) CCTV/VIDEO SURVEILLANCE WHERE THERE IS A REASONABLE EXPECTATION OF PRIVACY IN THE AREA TO BE VIEWED OR FOR THE INSTALLATION OF THE EQUIPMENT.

(U//FOUO) A warrant/court order is required for the use of CCTV/Video Surveillance when a reasonable expectation of privacy exists in either the area to be viewed or the location where the equipment will be installed, unless the installation and monitoring is being conducted pursuant to consent.

- A) (U//FOUO) **Criminal Investigations:** When there is a reasonable expectation of privacy in the area to be viewed and no consenting party, prior DOJ/OEO approval is required before seeking a warrant/order. When there is a reasonable expectation of privacy only in the location where the CCTV/Video Surveillance equipment will be installed, but not in the area to be viewed, prior DOJ/OEO authorization is not required to seek a warrant/order for the installation. In an emergency situation where CCTV usage is desired and a warrant/court order would be required, but cannot be obtained within the time required, an AUSA must be contacted to seek DOJ/OEO's guidance on how to proceed.
- B) (U//FOUO) **National Security Investigations:** The use of CCTV/Video Surveillance in national security investigations under the Foreign Intelligence Surveillance Act of 1978 (FISA) requires the filing of an appropriate FISA court order because the use of CCTV/Video Surveillance falls within the definition of "electronic surveillance" under FISA. See DIOG Section 18.7.3.
- C) (U//FOUO) **Where a warrant is required and the request is included with a Title III or is a FISA request:** Where the CCTV/video surveillance request is made pursuant to FISA or in conjunction with a Title III request, the required supervisory approvals and CDC or OGC review will take place as part of the larger FISA or Title III review and approval process. No additional reviews or approvals for the CCTV/video surveillance are required.
- D) (U//FOUO) **Where a warrant is required and the request is NOT coupled with a Title III request or made pursuant to FISA:** As the FD-759 is not used when a court order is needed, the required SSA approval and CDC or OGC review must be documented in an EC. A copy of the approving EC must be maintained in the field office ELSUR Subfile and a copy in the field office CCTV/Video Surveillance control file.

(U//FOUO) For additional information regarding the use of CCTV/Video Surveillance when a reasonable expectation of privacy exists, see the Video and Physical Surveillance Programs Policy Implementation Guide.

18.6.3.9 (U) COMPLIANCE AND MONITORING

(U//FOUO) Authorization documents regarding the use of the CCTV/Video Surveillance and electronic tracking devices (direction finders) must be documented in the investigative ELSUR file and will be available for compliance and monitoring review.

This Page is Intentionally Blank.

18.6.4 (U) INVESTIGATIVE METHOD: ADMINISTRATIVE SUBPOENAS (COMPULSORY PROCESS)

18.6.4.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//FOUO) Compulsory processes may be used to compel the disclosure of records and other tangible things relevant to an authorized investigation. Compulsory process in a Predicated Investigation includes, but is not limited to, the use of administrative subpoenas (as described below in this section); grand jury subpoenas (DIOG Sections 18.5.9 above and 18.6.5); trial subpoenas requested by the prosecuting attorney and issued by the trial judge; National Security Letters (NSL) (DIOG Section 18.6.6); and FISA Orders for business records (DIOG Section 18.6.7). Compulsory process is used to gather information in furtherance of FBI investigations. The FBI's authority to use such compulsory process is based upon Executive Branch delegated authorizations, statutes, regulations and the Federal Rules of Criminal Procedure (FRCP).

(U) An FBI CHS cannot be tasked to obtain records protected by the RFP, FCRA, ECPA, Buckley Amendment, except as specifically authorized by such law.

18.6.4.2 (U) APPLICATION

(U//FOUO) Administrative subpoenas may be used during certain predicated criminal investigations as authorized by statute. They may not be used for assistance to other agencies, unless their issuance is also relevant to an already open FBI Predicated Investigation as specified below.

18.6.4.3 (U) ADMINISTRATIVE SUBPOENAS

18.6.4.3.1 (U) SUMMARY

(U) The Attorney General has the authority to issue administrative subpoenas pursuant to two provisions of the United States Code, 21 U.S.C. § 876 and 18 U.S.C. § 3486. The FBI has no inherent authority to issue administrative subpoenas but has delegated authority from the Attorney General to do so. The use of administrative subpoenas is limited to three categories of investigations—drug program investigations, child sexual exploitation and abuse investigations, and health care fraud investigations—and may not be used for any other purpose. The delegated authority varies depending on the federal violation being investigated. The type of information that can be obtained using an administrative subpoena is also limited by law and by policy of the Attorney General.

(U//FOUO) Within the FBI, the authority to issue administrative subpoenas is limited to positions authorized by the Attorney General; that authority may not be further redelegated. This is an exception to the general delegation authority described in DIOG Section 3.4.C. An FBI employee properly designated to serve in an “acting” capacity in a position holding the delegation may issue an administrative subpoena. For issuing administrative subpoenas, relief supervisors may not exercise this authority during routine absences of the SSA or supervisory senior resident agent (SSRA) unless the SAC has specifically designated the relief

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§18

supervisor(s) as “acting” SSA or SSRA. All such “acting” designations must be in writing and appropriately retained as set forth in DIOG Section 3.4.

18.6.4.3.2 (U) LEGAL AUTHORITY AND DELEGATION

18.6.4.3.2.1 (U) INVESTIGATIONS INVOLVING THE SALE, TRANSFER, MANUFACTURE OR IMPORTATION OF UNLAWFUL DRUGS

(U) Authority: 21 U.S.C. § 876 and DOJ Regulation at 28 C.F.R. App to Pt. 0, Subpt. R § 4.

(U) May be issued to: Any individual or business holding records relevant to the drug investigation.

(U) Records to be obtained: Any records relevant or material to the investigation.

(U//FOUO) Delegated authority to issue: By DOJ regulation, the Attorney General’s delegation includes SACs, ASACs, SSRAs and “those FBI Special Agent Squad Supervisors who have management responsibilities over Organized Crime/Drug Program investigations.”

(U//FOUO) Multi-offense investigations: These administrative subpoenas may be issued for records relevant to an investigation regarding the sale, transfer, manufacture, or importation of unlawful drugs. On occasion, the drug offenses are being investigated with other offenses. In such instances, an administrative subpoena may only be issued for matters relevant to the drug investigation. The drug investigation may not be used as a subterfuge to use an administrative subpoena to obtain information that is not relevant to the drug investigation. If the information being subpoenaed has relevance to both the drug investigation and to the other aspects of the investigation, the information obtained with the administrative subpoena may properly be used in all aspects of the investigation.

(U//FOUO) Confidentiality: The recipient of an administrative subpoena is not prohibited from disclosing to the subject that records have been provided in response to an administrative subpoena. The Right to Financial Privacy Act limitations described in DIOG Section 18.6.4.1.4 applies. If an administrative subpoena is served on a provider of “electronic communication service” or a “remote computing service,” the provisions in the ECPA govern, as discussed in DIOG Section 18.6.4.1.4.

18.6.4.3.2.2 (U) INVESTIGATIONS INVOLVING THE SEXUAL EXPLOITATION OR ABUSE OF CHILDREN

(U) Authority: 18 U.S.C. § 3486(a) and Attorney General Order 3220-2010.

(U) May be issued to: A “provider of an electronic communication service” or a “remote computer service” (both terms defined below in DIOG Section 18.6.4.1.4.2.b) and only for the production of basic subscriber or customer information. The subpoena may require production as soon as possible but in no event less than 24 hours after service of the subpoena.

(U) **Records to be obtained:** Records relevant to the investigation are limited to the following specific subscriber information: customer or subscriber name; address; local and long distance connection records, or records of session times and durations; length of service (including start date) and types of service used; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address (this includes IP address); and means and source of payment for such service (including any credit card or bank account number).

(U//FOUO) **Delegated authority to issue:** ADICs, SACs, ASACs, SSRAs, Section Chiefs of the Criminal Investigative Division's (CID) Violent Criminal Threat Section and Cyber Division's (CyD) Strategic Outreach and Initiatives Section; the Unit Chiefs of CID's Crimes Against Children Unit and of CyD's Innocent Images National Initiative Unit and Innocent Images Operations Unit; those SSAs assigned to the Innocent Images Operations Unit with supervisory responsibility over assigned FBI personnel; those SSAs detailed to National Center for Missing and Exploited Children (NCMEC) with supervisory authority over assigned FBI personnel; and operational squad supervisors who have management responsibility over Innocent Images/Crimes Against Children programs.

(U//FOUO) **Violations to which this authority applies:** These administrative subpoenas may only be issued in investigations that involve a violation of 18 U.S.C. §§ 1201, 1591, 2241(c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 in which the victim is less than 18 years old. Under the Attorney General's delegation, an administrative subpoena in these investigations may be issued only to "providers of electronic communication services" or to "remote computing services" to obtain the information listed above. These administrative subpoenas may not be issued to any other person or entity or to obtain any other information, including the content of communications. There is no legal prohibition on the recipient of an administrative subpoena from disclosing to the subject that records have been provided in response to an administrative subpoena.

18.6.4.3.2.3 (U) INVESTIGATIONS INVOLVING FEDERAL HEALTH CARE FRAUD OFFENSES

(U) **Authority:** 18 U.S.C. § 3486(a)

(U) **Records to be obtained:** Records relevant to an investigation relating to a "federal health care offense." Federal health care offense is defined in 18 U.S.C. § 24.

(U) **May be issued to:** Any public or private entity or individual with records relevant to the federal health care offense. (These are referred to in guidance issued by the Attorney General as "investigative demands.")

(U//FOUO) **Delegated authority to issue:** The Attorney General has not delegated signature authority to the FBI. AG authority is delegated only to personnel within DOJ's Criminal Division and to United States Attorneys, who may redelegate the authority to AUSAs. FBI employees must request an AUSA to issue administrative subpoenas in health care fraud investigations.

(U) ***Limitations:*** The Right to Financial Privacy Act (RFPA) limitations described in paragraph D of this section apply. The provisions in ECPA govern, as discussed in paragraph D of this section, if the request for records is addressed to a “provider of electronic communication service” or a “remote computing service.” The subpoena may not require the production of records at a place more than 500 miles from the place the subpoena is served.

(U) There is no legal prohibition on the recipient of an administrative subpoena from disclosing to the subject that records have been provided in response to an administrative subpoena.

(U) ***Restriction on use of health care information against the individual:*** Pursuant to 18 U.S.C. § 3486, health information about an individual acquired through an authorized investigative demand may not be used in, or disclosed to any person for use in, any administrative, civil, or criminal action against that individual unless the action or investigation arises from and is directly related to receipt of health care, payment for health care, or a fraudulent claim related to health care.

18.6.4.3.3 (U) APPROVAL REQUIREMENTS

18.6.4.3.3.1 (U) REQUIRED FORM

- A) (U) An administrative subpoena must be prepared and issued using the electronic FD-1035 form (Administrative Subpoena) or a successor electronic form authorized for this purpose. The online form is designed to ensure an administrative subpoena is: (1) issued only in investigations where its use is permitted; (2) used to demand information that can be obtained within the applicable legal and policy limitations; and (3) signed by an individual with proper authority. The FD-1035 must be uploaded into the subpoena “SBP” subfile in the relevant investigative file from which it is issued. An electronic copy of the subpoena will automatically be saved in the FD-1035 data base when it is uploaded.
- B) (U) The FD-617 (Administrative Subpoena for Drug Program Investigations) and FD-909 (Administrative Subpoena for Child Sexual Exploitation/Abuse Investigations) remain temporarily available but their use is restricted to emergency situations when the FD-1035 is not available. Whenever the FD-617 or FD-909 is used, the legal requirements and the delegation authorities discussed above apply. Any subpoena issued using an FD-617, FD-909, or successor form must be uploaded into automated case support (ACS). Additionally, whenever the FD-617 or FD-909 is used, as soon as possible the FBI employee must also complete an FD-1035 using the identical information. The employee should not serve the subpoena generated by the FD-1035 but must attach it to the file copy of the FD-617 or FD-909 noting the date of service.
- C) (U) An FD-1035 administrative subpoena addressed to an electronic communication service provider contains an attachment explaining the meaning of various terms used in the demand for information. Some electronic communication service providers have adopted their own “riders” for use with subpoenas. These “riders” may not be used as an addition to any administrative subpoena issued by the FBI or proposed by the FBI for issuance by a DOJ attorney without approval from OGC or the CDC. That approval must be documented to the file.

18.6.4.3.3.2 (U) APPROVAL AUTHORITY

(U//FOUO) Use of an administrative subpoena requires SSA approval. The subpoena may be issued by the SSA if that SSA is among those with delegated authority to do so. See DIOG Sections 18.6.4.2.2.1 – 18.6.4.2.2.3 above) Otherwise, the subpoena must be forwarded to an individual with the proper delegated authority. Further review and approval may be required depending on the delegation. Review by the CDC is appropriate if legal questions arise in preparing and issuing the subpoena.

(U//FOUO) An individual designated by proper authority to serve in an “acting” status in one of the positions with delegated authority may sign and issue an administrative subpoena. The “acting” status must be documented in an appropriate field office administrative file. All such “acting” designations must be made in writing and appropriately retained as set forth in DIOG Section 3.4.3.2.

18.6.4.3.4 (U) LIMITATIONS ON USE OF ADMINISTRATIVE SUBPOENAS

18.6.4.3.4.1 (U) FINANCIAL PRIVACY LIMITATIONS

18.6.4.3.4.1.1 (U) OBTAINING RECORDS FROM A FINANCIAL INSTITUTION

(U//FOUO) “Financial records” are those records that pertain to a customer’s relationship with a financial institution. The term “financial institution” is broadly defined as a bank, savings bank, card issuer, industrial loan company, trust company, savings association, building and loan or homestead association, credit union, or consumer finance institution, located in any state, territory, or the District of Columbia. See 12 U.S.C. § 3401. (*Note:* The scope of the RFP’s definition of financial institution for this purpose, which limits the restrictions the RFP places on federal law enforcement in using an administrative subpoena, is narrower than the definition of financial institution that is used in connection with NSLs. For that purpose, the RFP refers to the broader definition found in the Bank Secrecy Act (BSA). Among the entities included in the BSA definition are money transmitting businesses, car dealers, travel agencies, and persons involved in real estate closings. See 12 U.S.C. § 3414(d) and 31 U.S.C. § 5312 (a)(2) and (c)(1).) When seeking financial records from a financial institution, the FBI must send a certificate of compliance required by 12 U.S.C. § 3403 to the financial institution. The certificate must indicate, among other things, that notice has been provided by the FBI to the individual customer whose financial records are to be obtained. The content of the notice is set out in 12 U.S.C. § 3405. A court order may be obtained that allows for delayed notice pursuant to 12 U.S.C. § 3409. Notice is not required if the administrative subpoena is issued to obtain the financial records of a corporation or for records not pertaining to a customer. Notice is also not required if the administrative subpoena seeks only basic account information, defined as name, address, type of account, and account number. See 12 U.S.C. § 3413(g).

18.6.4.3.4.1.2 (U) OBTAINING RECORDS FROM A CREDIT BUREAU

(U//FOUO) A credit bureau or consumer reporting agency may only provide name, address, former addresses, place of employment and former place of employment in response to an administrative subpoena. See 15 U.S.C. § 1681f. A credit bureau or consumer reporting agency may not release financial information in a credit report or consumer report, or the names and locations of financial institutions at which the consumer has accounts pursuant to an administrative subpoena. A court order, a grand jury subpoena, or, in an appropriate investigation, a national security letter may be used to obtain this information. 15 U.S.C. § 1681b. Notice of disclosure will be provided by the credit bureau or consumer reporting agency to the consumer if the consumer requests this information.

18.6.4.3.4.2 (U) ELECTRONIC COMMUNICATION PRIVACY ACT

(U//FOUO) The ability to gather subscriber information and the content of electronic communications using an administrative subpoena is governed by ECPA. In investigations involving the sexual exploitation or abuse of children, only basic subscriber or customer information may be obtained with an administrative subpoena under the terms of the Attorney General's delegation, as described above. No content information may be obtained. In drug and health care fraud investigations, an administrative subpoena may be used to obtain basic subscriber or customer information and certain stored communications, under limited circumstances, from entities that provide electronic communication services to the public.

18.6.4.3.4.2.1 (U) SCOPE

(U//FOUO) ECPA applies to two types of entities that provide electronic communications to the public. They are:

- A) "Electronic Communication Service" is defined as "any service that provides the user thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15)
- B) "Remote Computing Service" is defined as the "provision to the public of computer storage or processing service by means of an electronic communication system." 18 U.S.C. § 2711(12)

18.6.4.3.4.2.2 (U) SUBSCRIBER INFORMATION

(U//FOUO) The following information is available through administrative subpoena from entities that provide electronic communications to the public in the three categories of investigation described in DIOG Section 18.6.4.1.4.2. above:

- A) (U//FOUO) customer or subscriber name;
- B) (U//FOUO) address;
- C) (U//FOUO) local and long distance connection records or records of sessions, times, and duration;
- D) (U//FOUO) length of service (including start date) and types of service used;

- E) (U//FOUO) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address (this includes IP addresses); and
- F) (U//FOUO) means and source of payment for such service (including any credit card or bank account number).

(U//FOUO) Notice to the subscriber or customer is not required. The FD-1035 provides an attachment to explain these terms.

18.6.4.3.4.2.3 (U) SECOND GENERATION CONNECTION RECORDS

(U//FOUO) An administrative subpoena addressed to a provider of electronic communication services may not be used to simultaneously obtain “second generation connection records” along with the primary connection records. Second generation connection records are the connection records of the telephone or cell phone numbers called or received by the “seed” number—the primary number for which connection records are sought. These second generation records may also be referred to as a “community of interest” or “a calling circle based on a two-generation community of interest.” In order to obtain second generation connection records, a separate administrative subpoena must be issued after receipt of the first set of connection records. This second subpoena may only be issued if these additional connection records are relevant or material to the investigation. Subscriber identification information, if relevant, for the phone numbers may also be obtained using another subpoena.

18.6.4.3.4.2.4 (U) RECORDS OR OTHER INFORMATION PERTAINING TO A SUBSCRIBER

(U//FOUO) This is a larger category of information that includes any other records held by a service provider such as web surfing logs, buddy lists, cell-site data, and e-mail addresses in an address book. This information is not available through an administrative subpoena.

18.6.4.3.4.2.5 (U) CONTENT

(U//FOUO) Content is the actual substance of files stored in an account, including the subject line of an e-mail.

- A) (U) Unopened e-mail held in storage for 180 days or less may not be obtained using an administrative subpoena. A search warrant is required.
- B) (U) Unopened e-mail that has been held in electronic storage for more than 180 days may be obtained with an administrative subpoena. (In the Ninth Circuit, the opened e-mail and unopened e-mail must have been in storage for 180 days before it can be obtained with an administrative subpoena. See Theofel v. Farey-Jones, 359 F.3d 1066.) The government must provide notice to the subscriber or customer prior to obtaining such content. A limited exception to the notice requirement is provided in 18 U.S.C. § 2705.
- C) (U) E-mail that has been opened and the content of other electronically stored files held in storage by an entity that provides storage services to the public (i.e., a remote computing service, as defined in 18 U.S.C. § 2711), may be obtained using an administrative subpoena with notice to the customer or subscriber, unless notice is delayed in accordance with 18 U.S.C. § 2705.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

D) (U) E-mail that has been opened and the content of other electronically stored files held in storage by an entity that does not provide electronic communication services to the public, such as that on the internal network of a business, may be obtained using an administrative subpoena. Notice to the individual is not required because this demand is not restricted by ECPA.

(U) The FD-1035 administrative subpoena is not configured to obtain e-mail content because of developing case law in this area. This information may be obtain using an order issued under 18 U.S.C. § 2703(d). See DIOG Section 18.6.8.3.B.

18.6.4.3.4.3 (U) MEMBERS OF THE NEWS MEDIA

(U//FOUO) Approval Requirements: An administrative subpoena directed to a provider of electronic communication services or any other entity seeking to obtain local and long distance connection records, or records of session times of calls, made by a member of the news media may only be issued with the specific approval of the Attorney General. Before proposing such a subpoena, an agent should review 28 C.F.R. § 50.10. Requests for AG approval must be made by the AUSA involved in the investigation consistent with the DOJ policies set forth in 28 C.F.R. § 50.10. Guidance on the DOJ policy may be obtained from the Investigative Law Unit and/or the Privacy and Civil Liberties Unit, OGC.

18.6.4.3.5 (U) COMPLIANCE/MONITORING

18.6.4.3.5.1 (U) LIMITS ON USE

(U//FOUO) An administrative subpoena may only be issued for records that are relevant to investigations of controlled substances violations, sexual exploitation or abuse of children, or health care fraud. In health care fraud investigations, signature authority lies with DOJ. Administrative subpoenas may not be issued under any circumstance other than in support of the aforementioned investigations. Documents or records received as a result of the service of an administrative subpoena are not Rule 6(e) material and do not need to be handled like the information obtained by a FGJ Subpoena.

18.6.4.3.5.2 (U) OVERPRODUCTION

(U//FOUO) If any of the information that is obtained with an administrative subpoena is subject to statutory privacy protections (e.g., records subject to the Electronic Communications Privacy Act (ECPA), Right to Financial Privacy Act (RFPA), the Fair Credit Reporting Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA), or the Buckley Amendment), it must be reviewed at the time it is received by the employee who requested the issuance of an administrative subpoena to ensure that the information received from the third party provider is within the scope of the request. Any information received from a third party provider that is beyond the scope of the administrative subpoena and is subject to statutory protections must be treated as an overproduction. If it is determined that the overproduced material is subject to statutory protection, then the all of the produced material must be sequestered with the employee's supervisor and may not be uploaded into any FBI database or used in the investigation

until one the following methods of disposition have been completed at the discretion of the field office or FBIHQ division that issued the administrative subpoena:

- A) (U) The employee redacts the overproduced material. The employee's supervisor must approve the scope of the redaction. If there is any question whether the information provided is within the scope of the administrative subpoena, the CDC or OGC must be consulted. The method of redaction is left to the discretion of the employee, but redacted information must not be visible, used in the investigation, or uploaded into any FBI database. The method of redaction will vary depending on whether the information was provided in hard copy or electronically. After the overproduced information has been redacted, the remainder of properly produced information may be uploaded into any database and used in the investigation;
- B) (U) Another administrative subpoena has been served to address the overproduction. The field office or HQ division may serve a "curative" administrative subpoena if: (i) the investigation is still pending; (ii) the overproduced information is relevant to the investigation; and (iii) the FBI may lawfully obtain the overproduced information under statutory authority (i.e., the ECPA, RFP, etc.). After the "curative" administrative subpoena has been served, the FBI may immediately upload and use the sequestered information;
- C) (U) The records are returned to the entity that produced them; or
- D) (U) The records are destroyed.

(U) Whichever disposition is selected for the overproduction, it must be documented in the investigative subfile for administrative subpoenas.

(U) Any questions concerning this process, including the review or disposition of the responsive records, or the statutes which cover such records, should be discussed with the CDC or OGC.

18.6.4.3.5.3 (U) FACTORS FOR COMPLIANCE

(U//FOUO) The following factors should be considered to ensure compliance with applicable laws and regulations that govern the FBI's use of administrative subpoenas:

- A) (U//FOUO) The administrative subpoena must relate to a type of investigation for which the subpoena is authorized;
- B) (U//FOUO) The administrative subpoena must be directed to a recipient to whom an administrative subpoena is authorized;
- C) (U//FOUO) The administrative subpoena may request only records that are authorized under the pertinent law;
- D) (U//FOUO) The administrative subpoena must be approved by an authorized official;
- E) (U//FOUO) The administrative subpoena must be uploaded into the ACS system to the Subpoena ("SBP") subfile of the investigation for record purposes;
- F) (U//FOUO) The return of service information must be completed on the back of the original administrative subpoena;
- G) (U//FOUO) The original administrative subpoena and completed return of service must be maintained in a "SBP" subfile of the investigation; and

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§18

H) (U//FOUO) If the records provided in response to the administrative subpoena are subject to statutory privacy protections, they must be reviewed to ensure that they are within the scope of the request (i.e., that there is no overproduction). If an over-production has occurred, the procedures outlined above must be followed.

18.6.5 (U) INVESTIGATIVE METHOD: GRAND JURY SUBPOENAS (COMPULSORY PROCESS)

18.6.5.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//FOUO) Compulsory processes may be used to compel the disclosure of records and other information relevant to an authorized investigation; in addition, in a Type 1 & 2 Assessment, grand jury subpoenas may be used to obtain telephone or electronic mail subscriber information. Compulsory process in a Predicated Investigation includes, but is not limited to, the use of grand jury subpoenas (as described in this section below and in DIOG Section 18.5.9); administrative subpoenas (DIOG Section 18.6.4); trial subpoenas requested by the prosecuting attorney and issued by the trial judge; National Security Letters (NSL) (DIOG Section 18.6.6); and FISA Orders for business records (DIOG Section 18.6.7). Compulsory process is used to gather information in furtherance of FBI investigations. The FBI's authority to use such compulsory process is based upon Executive Branch delegated authorizations, statutes, regulations and the FRCP.

(U) An FBI CHS cannot be tasked to obtain records protected by the RFP, FCRA, ECPA, Buckley Amendment, except as specifically authorized by such law.

18.6.5.2 (U) APPLICATION

(U//FOUO) Grand jury subpoenas may be used during Predicated Investigations. This investigative method may not be used for assistance to other agencies, unless the assistance provided is also relevant to an already open FBI Predicated Investigation. A grand jury subpoena for telephone and electronic mail subscriber information only may be used in a Type 1 & 2 Assessment. A grand jury subpoena may not be used for the collection of positive foreign intelligence.

18.6.5.3 (U) FEDERAL GRAND JURY SUBPOENA

18.6.5.3.1 (U) LEGAL AUTHORITIES

(U) A Federal Grand Jury (FGJ) is an independent panel charged with determining whether there is probable cause to believe one or more persons committed a particular federal offense. If the FGJ believes probable cause exists, it will vote a "true bill" and the person will be indicted. An indictment is the most typical way a person is charged with a felony in federal court. A FGJ can collect evidence through the use of an FGJ subpoena, which is governed by Rule 6 of the FRCP. FRCP 6(e) controls the release of information obtained as part of the FGJ proceeding. FRCP 6(e) allows federal prosecutors to share foreign intelligence, counterintelligence, and terrorism-related threat information, and it is the DOJ's policy that such information should be shared to the fullest extent permissible by law and in a manner consistent with the rule. The Attorney General has issued revised Guidelines for the Disclosure and Use of Grand Jury Information under Rule 6(e)(3)(D) (hereinafter "FGJ-Guidelines"). A memorandum issued by the Deputy Attorney General on May 15, 2008, provides amplifying guidance.

18.6.5.3.2 (U) SCOPE

(U//FOUO) FGJ subpoenas can be used to demand documents, records, testimony of witnesses, or any other evidence deemed relevant by a sitting grand jury. The FBI can request the issuance of an FGJ subpoena in coordination with the responsible USAO in all criminal investigative matters. In Type 1 & 2 Assessments, telephone and electronic mail subscriber information may be requested through the use of an FGJ subpoena. An agent requesting a grand jury subpoena during an Assessment must advise the AUSA, who will issue the subpoena, that the FBI is conducting an Assessment. The AUSA must determine whether there is sufficient connection between the Assessment and possible criminal conduct to warrant issuance of a FGJ subpoena. FGJ subpoenas may not be sought during Type 3, 4, 5, or 6 Assessments. An FGJ subpoena may not be used in a positive foreign intelligence investigation. FGJ subpoenas are part of the investigative process. Thus, when an individual is indicted, further FGJ subpoenas may not be issued that are related to those offenses. Additional subpoenas pertaining to this individual could be issued, however, for any crimes that continue to be investigated and have not yet been indicted. FGJ subpoenas cannot be used to gather evidence for trial; trial subpoenas must be used for that purpose (see Rule 17 Federal Rules of Criminal Procedure).

18.6.5.3.3 (U) APPROVAL REQUIREMENTS

(U) There are no FBI supervisory approval requirements, but all FGJ subpoenas must be issued by the USAO that is handling the Type 1 & 2 Assessment or Predicated Investigation to which the subpoenaed materials or witnesses are relevant.

18.6.5.3.4 (U) DURATION OF APPROVAL

(U) FGJ subpoenas include a "return date," which is the date on which the subpoenaed materials or testimony is due to the grand jury.

18.6.5.3.5 (U) SPECIFIC PROCEDURES

(U) FGJ subpoenas are governed by Rule 6(e) of the Federal Rules of Criminal Procedure and can only be obtained in coordination with the responsible USAO or the appropriate DOJ division.

18.6.5.3.5.1 (U) MEMBERS OF THE NEWS MEDIA

(U) Approval Requirements: A grand jury subpoena directed to a provider of electronic communication services or any other entity seeking to obtain local and long distance connection records, or records of session times of calls, made by a member of the news media may only be issued with the specific approval of the Attorney General. Before proposing such a subpoena, an agent should review 28 C.F.R. § 50.10. Requests for AG approval must be made by the AUSA involved in the investigation consistent with the DOJ policies set forth in 28 C.F.R. § 50.10. Guidance on the DOJ policy may be obtained from the Investigative Law Unit and/or the Privacy and Civil Liberties Unit, OGC.

18.6.5.3.6 (U) NOTICE AND REPORTING REQUIREMENTS

(U) There is no FBI notice or reporting requirements for FGJ subpoenas.

18.6.5.3.7 (U) GRAND JURY PROCEEDINGS—GENERALLY

18.6.5.3.7.1 (U) PROCEDURAL ISSUES AND HANDLING OF FGJ MATERIALS

(U) The FGJ makes its determination whether to return a “true bill of indictment” based on evidence presented by the prosecuting attorney in an ex parte proceeding. The grand jury operates under the direction and guidance of the United States District Court. Generally, only witnesses for the prosecution testify before the grand jury.

(U) Only the United States Attorney or an assistant, other DOJ attorneys prosecuting the matter, the witness under examination, an interpreter (as needed), and the stenographer or operator of a recording device may be present while the grand jury is in session. No judge is present during the presentation of evidence although the court will sometime rule on evidentiary issues and will provide initial instructions to the FGJ. No person other than the grand jurors may be present while the grand jury is deliberating or voting.

18.6.5.3.7.2 (U) RESTRICTIONS ON DISCLOSURE

(U) As a general rule, no one other than a grand jury witness may disclose matters occurring before the grand jury. Government agents, even if called as witnesses, may not disclose matters occurring before the grand jury.

18.6.5.3.7.3 (U) EXCEPTIONS PERMITTING DISCLOSURE

18.6.5.3.7.3.1 (U) DISCLOSURES BY THE GOVERNMENT WITHOUT THE COURT’S PERMISSION

(U//FOUO) The government, through its attorney, may disclose grand jury matters under the following conditions:

- A) (U) Under Rule 6(e)(3)(A), the government may disclose a grand jury matter to certain persons in certain situations provided the government does not disclose the grand jury’s deliberations or any grand juror’s vote and the government provides the court that impaneled the grand jury with the names of all persons to whom disclosure was made and certifies that the government has advised the receiving party of the obligation of secrecy under this rule.
- B) (U) Persons eligible to receive material under this subsection are: 1) an attorney for the government for use in performing that attorney’s duty; 2) any government personnel, including state, local, tribal, or foreign government personnel that an attorney for the government considers necessary to assist in performing that attorney’s duty to enforce federal law; and 3) a person authorized under 18 U.S.C. § 3322.
- C) (U) For these purposes, OGC attorneys and CDCs are not “attorneys for the government.” For purposes of the Rules of Criminal Procedure, FRCP 1 defines “attorney for the government” as “the Attorney General, an authorized assistant of the Attorney General, a United States Attorney, [and] an authorized assistant of the United States Attorney.”

- D) (U) An attorney for the government may disclose any grand jury matter to another FGJ.
- E) (U) An attorney for the government may disclose any grand jury matter involving foreign intelligence, counterintelligence, or foreign intelligence information to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties. The government attorney must file, under seal, with the court that impaneled the grand jury, a notice that such information was disclosed and the agencies or departments that received the information. As used in Rule 6(e), foreign intelligence information is information that relates to the ability of the United States to protect against actual or potential attack or grave hostile acts by a foreign power or its agents; sabotage or international terrorism by a foreign power or its agents or clandestine intelligence activities by an intelligence service or network of a foreign power or its agents; or information with respect to a foreign power or foreign territory that relates to the national defense or security of the United States or the United States conduct of foreign affairs.
- F) (U) An attorney for the government may disclose any grand jury matter involving, either in the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent to any appropriate federal, state, local, tribal, or foreign government official for the purpose of preventing or responding to such threat or activities. The government attorney must file, under seal, with the court that impaneled the grand jury, a notice that such information was disclosed and the agencies or departments that received the information.

18.6.5.3.7.3.2 (U) DISCLOSURES BY THE GOVERNMENT REQUIRING THE COURT'S PERMISSION

(U//FOUO) The government, through its attorney, may disclose grand jury matters under the following conditions only with permission of the court. Petitions to make these disclosures are generally, but not always, filed with the court that impaneled the grand jury. Unless the hearing on the government's petition is to be ex parte, the petition must be served on all parties to the proceedings and the parties must be afforded a reasonable period of time to respond.

- A) (U) An attorney for the government may petition for disclosure to a foreign court or prosecutor for use in an official criminal investigation.
- B) (U) An attorney for the government may petition for disclosure to a state, local, tribal, or foreign government official, if the government attorney can show that the matter may disclose a violation of state, tribal, or foreign criminal law, and the purpose of the disclosure is to enforce that law.
- C) (U) An attorney for the government may petition for disclosure to an appropriate military official if the government attorney can show the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, and the purpose of the disclosure is to enforce that law.

18.6.5.3.7.3.3 (U) FBI'S CONDUIT RULE

(U//FOUO) Only the federal prosecutor is authorized to make an initial disclosure of Rule 6(e)(3)(D) foreign intelligence information. As a practical matter, such disclosures are ordinarily accomplished through the FBI, which may have existing information-

sharing mechanisms with authorized receiving officials. If the prosecutor intends to share information directly with another official, consultation with the FBI is required to ensure that disclosures will be consistent with the existing policy of intelligence community agencies and to ensure appropriate handling of sensitive or classified information. Disclosures to foreign officials should ordinarily be accomplished through the FBI, but there may be instances when sensitive information would be better protected in a foreign country if disclosure occurs through another intelligence agency.

(U//FOUO) If, in cases of emergency, the prosecutor must disclose information before consulting with the FBI, the prosecutor must notify the FBI as soon as practicable.

18.6.5.3.7.3.4 (U) OTHER LIMITATIONS

(U) Rule 6(e)(3)(D) does not eliminate certain other information protection requirements, such as restrictions on disclosure of tax returns and tax information, on certain financial information under the Right to Financial Privacy Act, and on classified information, to name only a few examples. Specific statutes may impose additional burdens of disclosures.

18.6.5.3.7.4 (U) DISCLOSURE

- A) (U) An FBI employee may become a "receiving official," i.e., the person to whom grand jury information can be disclosed, if the FBI receives grand jury information developed during investigations conducted by other agencies. A receiving official is any federal, state, local, tribal, or foreign government official receiving grand jury information, disclosed by an attorney for the government, under any provision of Rule 6(e)(3)(D). A receiving official may only use the disclosed material as necessary in the conduct of his/her official duties. The receiving official ordinarily must consult with the federal prosecutor before disseminating the information publicly, including in open court proceedings.
- B) (U//FOUO) Receiving officials may only use grand jury information in a manner consistent with FGJ Guidelines and any additional conditions placed on the use or handling of grand jury information by the attorney for the government.
- C) (U//FOUO) If dissemination is necessary to the performance of his or her official duties, a receiving official may disseminate Rule 6(e)(3)(D) information outside of that official's agency to other government officials.
- D) (U) A receiving official, other than a foreign government official, must consult with the attorney for the government before disseminating Rule 6(e)(3)(D) information publicly (including through its use in a court proceeding that is open to or accessible to the public), unless prior dissemination is necessary to prevent harm to life or property. In such instances, the receiving official shall notify the attorney for the government of the dissemination as soon as practicable.
- E) (U) A foreign government receiving official must obtain prior consent from the disclosing official where possible, or if the disclosing official is unavailable, from the agency that disseminated the information to that foreign official before dissemination of the information to a third government or publicly. Public dissemination includes using the information in a court proceeding that is open to or accessible by the public.

- F) (U) A receiving official shall handle Rule 6(e)(3)(D) information in a manner consistent with its sensitivity and shall take appropriate measures to restrict access to this information to individuals who require access for the performance of official duties.
- G) (U) A receiving official shall immediately report to the disclosing attorney for the government: any unauthorized dissemination of Rule 6(e)(3)(D) information; or any loss, compromise, or suspected compromise of Rule 6(e)(3)(D) information.

18.6.5.3.7.4.1 (U) VIOLATIONS

- A) (U) A receiving official who knowingly violates Rule 6(e)(3)(D) by using the disclosed information outside the conduct of his or her official duties, or by failing to adhere to any limitations on the dissemination of such information, may be subject to contempt of court proceedings and to restriction on future receipt of Rule 6(e)(3)(D) information.
- B) (U) A state, local, tribal, or foreign government official who receives Rule 6(e)(3)(D) information, and who knowingly violates these guidelines, may be subject to contempt of court proceedings.
- C) (U) An attorney for the government who knowingly violates Rule 6(e)(3)(D) may be subject to contempt of court proceedings.

18.6.5.3.7.4.2 (U) LIMITATION ON UNAUTHORIZED DISCLOSURES

(U) Rule 6(e)(3)(D)(i) provides that receiving officials may use disclosed information only to conduct their “official duties subject to any limitation on the unauthorized disclosure of such information.” This “limitation on unauthorized disclosures” is understood to encompass applicable statutory, regulatory, and guideline restrictions regarding classification, privacy, or other information protection, as well as any additional restrictions imposed by the federal prosecutor.

(U//FOUO) The FGJ Guidelines do not require the receiving official to notify the federal prosecutor of subsequent disclosures, except for consultation concerning public disclosures and consent for certain disclosures by foreign officials. The receiving official is bound by whatever restrictions govern his or her use and disclosure of the information as part of his official duties. (Memo dated 5/15/08, Guidelines for the Disclosure and Use of FGJ Information under Rule 6(e)(3)(D)).

18.6.5.3.7.4.3 (U) LIMITATION OF USE

- A) (U//FOUO) Because of the restrictions involved in handling information that is obtained by the use of a grand jury subpoena, whenever possible, alternatives to the grand jury subpoena, such as administrative subpoenas, search warrants and witness interviews should be considered as an alternative method of obtaining evidence.
- B) (U) A grand jury subpoena may only be used for purposes of gathering information that is relevant to the grand jury’s investigation. Grand jury secrecy continues indefinitely, regardless of whether there is an indictment, unless the material becomes a matter of public record, such as by being introduced at trial.
- C) (U) Rule 6(e)(3)(D) does not require notice to the court of subsequent dissemination of the information by receiving officials.

- D) (U//FOUO) Disclosure of grand jury material cannot be made within the FBI for unrelated investigations unless a government attorney has determined that such disclosure to a particular investigator is needed to assist that attorney in a specific criminal investigation. The ability of government attorneys to freely share grand jury material with other government attorneys for related or unrelated criminal investigations does not extend to investigators without investigation specific authorization from the government attorney and notice to the court. **Therefore, grand jury material must be restricted when placed into a general system of records that is freely accessible to FBI employees and others with access (e.g., ACS).**
- E) (U//FOUO) If a government attorney authorizes the disclosure of grand jury material in the possession of the FBI for use in an unrelated federal criminal matter, such approval must be documented in the grand jury subfile of both the initiated investigation file and the subsequent investigation file. That documentation will be in addition to any necessary supplementation to the government attorney's FRCP Rule 6(e) disclosure letter and/or to the internal disclosure list.
- F) (U//FOUO) The USAO should be consulted immediately for precautionary instructions if grand jury material will have application to civil law enforcement functions (e.g., civil RICO or civil forfeiture). There are very limited exceptions that allow government attorneys to use grand jury material or information in civil matters (e.g., civil penalty proceedings concerning banking law violations). These exceptions do not automatically apply to investigative personnel. Therefore, any similar use of grand jury information by the FBI must be approved in advance by the government attorney.
- G) (U//FOUO) Disclosure cannot be made without a court order for use in non-criminal investigations, such as background investigations or name checks.
- H) (U//FOUO) Government personnel who are preparing a response to a Freedom of Information Act or Privacy Act request may properly access grand jury material under the Rule because they are considered to be assisting the grand jury attorney by ensuring against any improper disclosure.

18.6.5.3.7.4.4 (U) MATTERS OCCURRING BEFORE THE GRAND JURY

- A) (U) **Core Grand Jury Material:** There can be no dissemination of matters occurring before the grand jury unless such dissemination comes within one of the exceptions discussed above. There is no uniform legal definition of what constitutes matters occurring before the grand jury except for what is generally referred to as "core" grand jury material. "Core grand jury material" includes the following: (i) names of targets and witnesses; (ii) grand jury testimony; (iii) grand jury subpoenas; (iv) documents with references to grand jury testimony (including summaries and analyses); (v) documents that clearly reveal the intentions or direction of the grand jury investigation; and (vi) other material that reveals the strategy, direction, testimony, or other proceedings of a grand jury.
- B) (U) **Documents Created Independent of Grand Jury but Obtained by Grand Jury Subpoena:** Rule 6(e) generally prohibits disclosing "matters occurring before the grand jury." The rule, however, does not define that phrase. The issue of whether pre-existing documents fall within that prohibition has never been settled conclusively by the Supreme Court, although many lower courts have discussed it at length. Courts generally agree that this prohibition does not cover all information developed in the course of a grand jury investigation; rather, the secrecy rule applies only to information that would reveal the existence, strategy or direction of the grand jury investigation, the nature of the evidence produced before the grand jury, the views expressed by members of the grand jury, or anything else that actually occurred before the grand jury. In addition, courts have frequently held that Rule 6(e) does not protect documents

subpoenaed by the government from third parties only for the information contained within the document rather than to determine the direction or strategy of the grand jury investigation. Due to developing law on this issue, FBI personnel should consult with the AUSA responsible, or the CDC/OGC, to determine how best to handle such documents.

- C) (U//FOUO) ***Data Extracted from Records Obtained by Grand Jury Subpoena***: Information extracted from business records that were obtained by grand jury subpoena is often used to facilitate investigations. Some of that type of data is, by statute or case law, subject to grand jury secrecy rules. In other investigations, determination of whether data must be considered subject to grand jury secrecy rules depends on the case law and local practice in the federal district. Information extracted from grand jury subpoenaed financial records subject to the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3420) must be treated as grand jury material “unless such record has been used in the prosecution of a crime for which the grand jury issued an indictment or presentment or for a purpose authorized by rule 6(e) of the Federal Rules of Criminal Procedure.” (emphasis added). Rule 6(e)(3)(B) authorizes grand jury material to be used “to assist an attorney for the government in performing that attorney’s duty to enforce federal criminal law.” Use of information obtained through a grand jury subpoena by FBI employees to advance an investigation does not constitute a disclosure of grand jury information in violation of Rule 6(e). With the approval of the USAO, information from subpoenaed telephone records may be disclosed for use in unrelated federal criminal investigations in those districts where such material is not considered a “matter occurring before a grand jury.” If the USAO approves generally of this procedure, such information may be used in unrelated criminal investigations without authorization from a government attorney in each instance.

18.6.5.3.7.4.5 (U) FEDERAL GRAND JURY PHYSICAL EVIDENCE AND STATEMENTS OF WITNESSES

- A) (U) Physical evidence provided to the government in response to a grand jury subpoena is subject to the secrecy rule regardless of whether such evidence is presented to the grand jury. Physical evidence provided voluntarily or obtained by means other than grand jury process (such as by consent or a search warrant) is not a grand jury matter regardless of whether such evidence was previously or is thereafter presented to the grand jury. The fact that the physical evidence was presented to the grand jury is, however, subject to the grand jury secrecy rules.
- B) (U) Statements of witnesses obtained as a result of grand jury process including grand jury subpoena, such as a statement given in lieu of grand jury testimony, are matters occurring before the grand jury irrespective of whether such witnesses testified before the grand jury or are not required to testify. Voluntary statements of witnesses made outside of the grand jury context (not pursuant to any grand jury process including a grand jury subpoena), including statements made outside the grand jury by a witness who is being prepared for grand jury testimony, are not grand jury matters irrespective of whether the witness previously testified or will thereafter testify before the grand jury.
- C) (U) Rule 6(e)(3)(B) requires a federal prosecutor who discloses grand jury material to government investigators and other persons supporting the grand jury investigation to promptly provide the court that impaneled the grand jury the names of the persons to whom such disclosure has been made and to certify that he/she has advised such persons of their obligation of secrecy under the Rule. In order to document the certification required by the Rule, government attorneys often execute and deliver to the court a form, normally referred to as a “Certification” or “Rule 6(e) letter.” A copy of this document should be maintained with the grand jury material held in the FBI’s custody.

- D) (U//FOUO) ***Documentation of Internal Disclosures of Grand Jury Material:*** Grand jury material should be kept in such as fashion as to maintain the integrity of the evidence. Upon taking custody of grand jury material, the FBI employee should categorize it in a manner to identify its production source and how it was obtained, to include the identity of a custodian of record for documentary evidence. Practical considerations often require agents assisting government attorneys to seek assistance in the same investigation from others within the FBI. In many districts, support personnel and supervisors of case agents need not be routinely included in the list provided to the court. In lieu of a Rule 6(e) letter from the USAO containing an exhaustive list of names of FBI personnel, an FBI record of additional internal disclosures must be maintained by the case agent in order to establish accountability. Use of this "internal certification" procedure should be authorized by the appropriate USAO. The internal form must record the date of disclosure as well as the identity and position of the recipient. Such internal disclosures may be made only in support of the same investigation in which a federal prosecutor has previously issued a Rule 6(e) letter. In addition, the internal record must reflect that all recipients of grand jury materials were advised of the secrecy requirements of Rule 6(e). Whenever practicable, recipients should be listed on this internal certification prior to disclosure. Local Rule 6(e) customs should govern the internal certification process used.
- E) (U//FOUO) ***Storage of Grand Jury Material:*** The FBI cannot make or allow unauthorized disclosure of grand jury material. Material and records obtained pursuant to the grand jury process are frequently stored in FBI space. FBI personnel should report any unauthorized disclosure to the appropriate government attorney who, in turn, must notify the court. In order to protect against unauthorized disclosure, grand jury material must be secured in the following manner:
- 1) (U//FOUO) The cover, envelope, or container containing grand jury materials must be marked with the warning: "GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e)." No grand jury stamp or mark should be affixed to the original material. Agents, analysts and other authorized parties should work from copies of grand jury material whenever possible to ensure the original material retains its integrity.
 - 2) (U//FOUO) Access to grand jury material must be limited to authorized persons (e.g., those assisting an attorney for the government in a specific criminal investigation). All necessary precautions should be taken to protect grand jury material, to include maintaining the material in a secure location when not in use. The material must be appropriately segregated, secured, safeguarded and placed in the investigative subfile for FGJ material. Absent chain-of-custody considerations, grand jury material may be maintained in the 1A section of the file. Grand jury material need not be kept in an evidence or bulky exhibit room and may be entrusted to a support services technician (SST) or evidence control technician (ECT). Should grand jury material be entered into a computer database, the data must be marked with the 6(e) warning and restricted within the system.
 - 3) (U//FOUO) Registered mail or other traceable courier (such as Federal Express) approved by the Chief Security Officer (CSO) must be used to mail or transmit to other field offices any documents containing grand jury material. Couriers and other personnel employed in these services will not be aware of the contents of the material transmitted because of the wrapping procedures specified below, and therefore, then do not require a background investigation for this purpose. The names of persons who transport the material need not be placed on a disclosure list, but the receiving office must provide the case agent in the originating office with the names of personnel in the receiving office to whom disclosure is made.

- 4) (U//FOUO) Grand jury material that is to be mailed or transmitted by traceable courier outside a facility must be enclosed in opaque inner and outer covers. The inner cover must be a sealed wrapper or envelope that contains the addresses of the sender and the addressee, who must be authorized to have access to the grand jury material. The inner cover must be conspicuously marked "Grand Jury Information To Be Opened By Addressee Only." The outer cover must be sealed, addressed, return addressed, and bear no indication that the envelope contains grand jury material. When the size, weight, or nature of the grand jury material precludes the use of envelopes or standard packaging, the material used for packaging or covering must be of sufficient strength and durability to protect the information from unauthorized disclosure or accidental exposure.
- 5) (U//FOUO) If the government attorney determines that the sensitivity of, or threats to, grand jury material necessitates a more secure transmission method, the material may be transmitted by an express mail service approved for the transmission of national security information or be hand carried by the assigned government attorney or his or her designated representative.
- 6) (U//FOUO) Grand jury material containing classified national security information must be handled, processed, and stored according to 28 C.F.R. Part 17. Grand jury material containing other types of sensitive information, such as federal tax return information, witness security information, and other types of highly sensitive information that have more stringent security requirements than that usually required for grand jury material must be stored and protected pursuant to the security regulations governing such information and any special security instructions provided by the organization that originated the information.
- 7) (U//FOUO) Original documents that are obtained through the grand jury process should be returned to the attorney for the government or, with the government attorney's permission, to the owner if there is no indictment or the prosecution has concluded.

18.6.5.3.7.4.6 (U) REQUESTS FOR SUBPOENAS IN FUGITIVE INVESTIGATIONS

(U//FOUO) The function of the grand jury is to decide whether a person should be charged with a federal crime. Locating a person who has been charged is a task that is ancillary to, rather than a part of, that function. As such, grand jury subpoenas cannot be used as an investigative aid in the search for a fugitive in whose testimony the grand jury has no interest. Absent one the exceptions discussed below being applicable, grand jury subpoenas for testimony or records related a fugitive's whereabouts may not be requested in FBI fugitive investigations.

(U//FOUO) If the grand jury has a legitimate interest in the testimony of a fugitive regarding an ongoing investigation, it may subpoena other witnesses and records in an effort to locate the fugitive. In this situation, the responsible Assistant Attorney General must approve a "target" subpoena for the fugitive before the grand jury may subpoena witnesses and records to locate the fugitive.

(U//FOUO) When a fugitive's present location is relevant to an offense under investigation, the grand jury may legitimately inquire as to the fugitive's whereabouts. Offenses such as harboring, misprision of a felony, and accessory after the fact are examples of crimes as to which the fugitive's location may be relevant evidence. If, however, the person who is suspected of harboring the fugitive or being an accessory

after the fact has been immunized and compelled to testify regarding the location of the fugitive, this will likely be viewed as improper subterfuge.

(U//FOUO) DOJ policy generally forbids the use of grand jury subpoenas to locate a defendant charged in a federal criminal complaint with unlawful flight to avoid prosecution (UFAP). UFAP investigations are, as a general rule, not prosecuted. Use of the grand jury in the investigation of a UFAP matter requires prior consultation with DOJ and written authorization to prosecute from the Assistant Attorney General in charge of the Criminal Division. Federal indictments for UFAP require prior written approval of the Attorney General, Deputy Attorney General, or an Assistant Attorney General.

18.6.5.3.7.5 (U) OVERPRODUCTION

(U) If any of the information received in response to a FGJ subpoena is subject to statutory privacy protections (e.g., records subject to the Electronic Communications Privacy Act (ECPA), Right to Financial Privacy Act (RFPA), the Fair Credit Reporting Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA), or the Buckley Amendment), it must be reviewed at the time it is received by the employee who requested the issuance of the FGJ subpoena to ensure that the information received is within the scope of the subpoena's demand. Any information received from a third party provider that is beyond the scope of the FGJ subpoena and is subject to statutory protections must be treated as an overproduction. Overproduced material must not be uploaded into any FBI application database or used in any manner. Instead, the FBI employee must promptly notify the AUSA who authorized the issuance of the FGJ Subpoena of the potential overproduction. The AUSA, in coordination with the FBI employee, must determine whether the information exceeds the scope of the FGJ subpoena, and if so, how to dispose of the overproduced material. Whatever disposition of the overproduction is chosen it must be documented in the investigative subfile for FGJ subpoenas.

This Page is Intentionally Blank.

18.6.6 (U) INVESTIGATIVE METHOD: NATIONAL SECURITY LETTER (COMPULSORY PROCESS)

18.6.6.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//FOUO) Compulsory processes may be used to compel the disclosure of records and other information relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Compulsory process in a Predicated Investigation includes, but is not limited to, the use of National Security Letters (NSL) (described below in this section); grand jury subpoenas (DIOG Sections 18.6.5 and 18.5.9); administrative subpoenas (DIOG Section 18.6.4); trial subpoenas requested by the prosecuting attorney and issued by the trial judge; and FISA business records orders (DIOG Section 18.6.7). Compulsory process is used to gather information in furtherance of FBI investigations. The FBI's authority to use such compulsory process is based upon Executive Branch delegated authorizations, statutes, regulations and the FRCP.

(U) An FBI CHS cannot be tasked to obtain records protected by the RFP, FCRA, ECPA, Buckley Amendment, except as specifically authorized by such law.

18.6.6.2 (U) APPLICATION

(U//FOUO) National Security Letters (NSLs) may be used in a national security Predicated Investigation. This method may not be used for assistance to other agencies, unless relevant to an already open FBI authorized investigation.

18.6.6.3 (U) NATIONAL SECURITY LETTERS

18.6.6.3.1 (U) LEGAL AUTHORITY

- A) (U) 12 U.S.C. § 3414(a)(5)(A);
- B) (U) 15 U.S.C. §§ 1681u and 1681v;
- C) (U) 18 U.S.C. § 2709;
- D) (U) 50 U.S.C. § 436;
- E) (U) AGG-Dom, Part V; and
- F) (U) A National Security Letter (NSL) may be used only to request:
 - 1) (U) Financial Records: The Right to Financial Privacy Act (RFP), 12 U.S.C. § 3414(a)(5);
 - 2) (U) Identity of Financial Institutions: Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u(a);
 - 3) (U) Consumer Identifying Information: FCRA, 15 U.S.C. § 1681u(b);
 - 4) (U) Identity of Financial Institutions and Consumer Identifying Information: FCRA, 15 U.S.C. §§ 1681u(a) and (b);
 - 5) (U) Full Credit Reports in International Terrorism Investigations: FCRA, 15 U.S.C. § 1681v; and

- 6) (U) Telephone Subscriber Information, Toll Billing Records, Electronic Communication Subscriber Information, and Electronic Communication Transactional Records: Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709.

18.6.6.3.2 (U) DEFINITION OF METHOD

(U) A National Security Letter (NSL) is an administrative demand for documents or records that are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Sample NSLs are available. NSLs may not be issued in an Assessment.

18.6.6.3.3 (U) APPROVAL REQUIREMENTS

(U//FOUO) The process for creating an NSL involves two documents: the NSL itself and the EC approving the issuance of the NSL. The authority to sign NSLs has been delegated to the Deputy Director, Executive Assistant Director, and Associate EAD for the National Security Branch; Assistant Directors and all DADs for CT/CD/Cyber; General Counsel; Deputy General Counsel for the National Security Law Branch; Assistant Directors in Charge in NY, WFO, and LA; and all SACs. This delegation includes FBI officials properly designated to serve in these positions in an acting capacity. No other delegations are permitted. The following requirements for designating an acting official are particular to NSLs and are more restrictive than the Succession and Delegation Policy set forth in DIOG Section 3:

- A) (U//FOUO) When traveling on official orders outside the geographical limits of the field office or division, on leave, or otherwise unavailable to fulfill the duties of their positions: ADICs and SACs may designate an immediate subordinate, no lower than an ASAC as Acting ADIC or SAC (respectively); and HQ officials may designate a subordinate no lower than a Section Chief as Acting AD or DAD. Such designations must be documented in 319X-HQ-A1565545-XX in which the last two alpha characters designate the office, division, or Legat. See DIOG Section 3.4.3.3.
- B) (U//FOUO) Those designated as acting officials for purposes of signing NSLs must be properly trained on NSL policies as set forth in Corporate Policy Notice 0227N. Any designation must be made in writing with notice to the supervisory ADIC (if any) or to the Deputy Director. In addition, a hard copy of such standing orders must be forwarded to the supervisory ADIC (if any) or to the Deputy Director. The designation may be accomplished by a record email or EC, expressly stating the date on which the acting official's authority becomes effective. All such emails or ECs must be uploaded and maintained in an appropriate control file in the office in which the acting official is acting.
- C) (U//FOUO) ADICs, SACs, and HQ officials may also choose to document by EC a "standing order of succession," which automatically takes effect when they are traveling, absent, or unavailable. The EC documenting the standing order of succession must be approved by that official, or if unavailable, by the Deputy Director, and uploaded and maintained in the appropriate administrative file as set forth in Section 3.4.3. The EC must indicate under what circumstances the standing order of succession takes effect.
- (U) Additional details and instructions can be found in Corporate Policy Notice 0227N.

(U//FOUO) In addition to being signed by a statutorily-required approver, every NSL must be reviewed and approved by a CDC, ADC (or attorney acting in that capacity), or an NSLB attorney.

18.6.6.3.4 (U) STANDARDS FOR ISSUING NSLS

(U) The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is that the material sought is relevant to an authorized investigation to protect against international terrorism or clandestine activities, provided that such an investigation of an USPER is not predicated solely on activities protected by the First Amendment of the Constitution of the United States. Thus, an NSL may not be issued unless the information sought is relevant to an open and authorized Preliminary Investigation (PI) or Full Investigation (Full). **NSLs may not be issued in an Assessment. (An NSL request for a full credit report is not available in counterintelligence investigations unless there is an international terrorism nexus. 15 U.S.C. § 1681v.)**

(U//FOUO) Information is relevant if it tends to make a fact more or less probable. In the context of NSLs, there must be a reasonable belief that the information sought through the NSL either supports or weakens facts being investigated in an investigation. For example, financial records believed to support a subject's assertion that he or she was in the United States at a given time when the FBI believes he or she was outside the United States are relevant to the investigation because they tend to exculpate the subject. On the other hand, phone records of a sibling of a subject of an investigation not known to be in contact with the subject would not, barring additional information, be relevant to the national security investigation.

(U//FOUO) In addition to the information being relevant, the investigation of an USPER cannot be conducted solely based on activities protected by the First Amendment. For example, the FBI cannot issue an NSL for phone records of an individual solely because the individual attends a mosque that is also attended by international terrorism (IT) subjects. The individual's attendance at a place of worship is First Amendment-protected activity, on which the FBI cannot base an investigation. On the other hand, if the FBI reasonably believes that, in addition to attending the same mosque as the IT subjects, the individual received money transfers from IT subjects, then an NSL seeking his or her phone or bank records would be relevant to a national security investigation and would not be based solely on First Amendment-protected activities.

(U//FOUO) The EC that requests the issuance of an NSL must provide a sufficiently detailed explanation of the predication for the investigation and the relevance of the material sought by the NSL so that a meaningful review can be conducted. The information necessary to make a judgment regarding predication and relevance should be contained in the four corners of the EC. If the necessary information cannot be included in the EC because, for example, the information is classified Top Secret or the investigation involves insider espionage, the EC should clearly reference the source document that provides the predication and explain why the underlying information cannot be included in the EC.

(U//FOUO) Approval of an NSL must include a review of the predication of the underlying investigation. Although there is no legal review for opening an investigation, there must be a

review of the predicate for the investigation in determining whether an NSL request meets the legal standard of the relevant statutory authority.

(U//FOUO) As with all investigative methods, before requesting an NSL, the employee initiating the request should consider whether an NSL is the least intrusive and reasonable means based upon the circumstances of the investigation to obtain the needed information. See DIOG Section 4.4.

18.6.6.3.5 (U) SPECIAL PROCEDURES FOR REQUESTING COMMUNICATION SUBSCRIBER INFORMATION

(U//FOUO) If only subscriber information is needed for an investigation, an NSL should be issued for subscriber records rather than a broader request for subscriber and toll billing/transactional records.

(U//FOUO) Generally, all toll billing/transactional records responsive to the NSL may be uploaded into FBI databases. Before issuing NSLs seeking to identify a subscriber of facilities contained in such toll/transactional records, the employee should determine whether the identities of the subscribers of some or all of the telephone numbers/email accounts identified in the toll billing/transactional records are needed to advance the investigation. If so, the employee may issue subsequent NSLs to identify the subscriber(s) of such telephone numbers or email accounts. NSLs should not be used to identify the subscribers of numbers or email accounts if that information is not needed to advance the investigation and should not be issued unless and until that identity becomes needed for the investigation or some other investigation.

(U//FOUO) If a subscriber's identity may contribute to the investigation, the investigator should also consider whether an NSL is the least intrusive and reasonable means to obtain the information. In some instances, information obtained from open source or government databases may be sufficient to meet investigative needs. The information obtained from such sources may not be current or accurate; however, those factors, among others, should be considered in determining whether to issue an NSL.

18.6.6.3.6 (U) DURATION OF APPROVAL

(U) The authority for an NSL remains valid until the information requested is fulfilled.

18.6.6.3.7 (U) SPECIFIC PROCEDURES

(U//FOUO) A cover EC that documents the relevance of the information sought and the need for non-disclosure (if a non-disclosure provision is included in the NSL) must accompany all NSLs. All NSLs, with limited exceptions discussed below, must be created on the NSL subsystem to the FISA Management System (FISAMS). The EC must reference an investigative file—not a control file—to which the information sought is relevant.

(U//FOUO) The NSL subsystem allows for the web-based creation of NSLs and supporting ECs. Use of the subsystem ensures that the information in the NSL is consistent with the

supporting EC, the appropriate statutory authority is cited, and the necessary approvals are obtained.

(U//FOUO) Under the following circumstances only, NSLs may be created outside the NSL subsystem:

- A) (U//FOUO) **NSLs seeking second-generation/community of interest information:** These NSLs require specific language and require a demonstration of the relevance of the second-generation information to the investigation. This type of NSL request is used rarely and is a subset of NSLs served by the Communications Analysis Unit (CAU). This type of NSL is not yet available in the NSL subsystem. Such NSLs may only be created outside the NSL subsystem with prior approval from the Deputy General Counsel (DGC) of the National Security Law Branch (NSLB). The DGC's approval must be documented in the EC authorizing the NSL.
- B) (U//FOUO) **Time sensitive situations:** If there is an emergency or other time sensitive matter in which not all approvals required in the NSL subsystem can be timely completed or technical issues pose a barrier to using the NSL subsystem, the NSL and EC may be created outside the NSL subsystem. The EC authorizing the NSL must explain why the NSL is "time sensitive."
- C) (U//FOUO) **Insider espionage investigations:** Sensitive insider espionage investigations may justify the creation of NSLs outside the NSL subsystem. Such NSLs may only be created outside the NSL subsystem with prior approval from the DGC of NSLB or an NSLB Section Chief. The approval of the NSLB DGC or Section Chief must be documented in the EC authorizing the NSL.
- D) (U//FOUO) **NSLs requiring specific limiting language:** Such NSLs may only be created outside the NSL subsystem with prior approval from the DGC of NSLB or an NSLB SC. The approval of the NSLB DGC or Section Chief must be documented in the EC authorizing the NSL.
- E) (U//FOUO) **Curative NSLs:** These NSLs are issued to provide authority to retain information already provided in response to an earlier NSL. The EC authorizing the NSL must state that the NSL is a "curative NSL" and include a brief explanation why a curative NSL is necessary.
- F) (U//FOUO) **NSLs containing non-standard language:** These NSLs seek, for example, a specific bank record rather than all financial records in the bank's possession, or a specific type of electronic communication transactional record rather than all transactional records. Such NSLs may only be created outside the NSL subsystem with the prior approval of the DGC of NSLB, an NSLB SC, or the Unit Chief of the National Security Law Policy and Legislative Review Unit of NSLB. The NSLB's approval must be documented in the EC authorizing the NSL.

(U//FOUO) NSLs created outside the NSL subsystem **must** be created using the model NSLs and ECs available on the [NSLB website](#). In every case in which an NSL is created outside the NSL subsystem, the EC approving the issuance of that NSL **must** include the following information: (i) the reason the NSL was created outside the NSL subsystem; and (ii) if prior approval was required, from whom it was obtained. Such NSLs **must** contain a lead to NSLB so that information needed for Congressional reporting purposes can be recorded, as well as a lead to the relevant HQ operational unit for informational purposes.

(U//FOUO) No later than ten (10) days after the issuance of an NSL outside the NSL subsystem, both the NSL and EC must be uploaded to ACS (unless otherwise exempted from uploading into ACS), as well as forwarded via email to NSLB at the following email address: HQ_DIV09_NSL_REPORTING. If the investigation involves a particularly sensitive matter that precludes emailing the NSL and/or EC, then a separate EC, containing notice of the sensitivity and the statistical information needed for tracking NSLs, must be sent to the DGC of NSLB.

(U//NFOUO) Any question concerning whether an NSL may be created outside the NSL subsystem must be directed to NSLB.

(U//FOUO) For additional information regarding seeking subscriber identifying information, see the Attorney General approved Procedures for the Collection, Use, and Storage of Information Derived from National Security Letters.

18.6.6.3.7.1 (U) COVER EC

(U//FOUO) The EC must reference an investigative file—not a control file—to which the information sought is relevant.

(U//FOUO) If non-disclosure of the NSL is sought, the EC must set forth the factual predicate for imposing non-disclosure. The certification supporting a non-disclosure obligation must assert that disclosure may endanger national security; interfere with a criminal, counterterrorism, or counterintelligence investigation; interfere with diplomatic relations; or endanger the life or safety of any person. Accordingly, the EC must establish why any of those dangers may arise from disclosure of the NSL. Possibilities include:

- A) (U//FOUO) Disclosure may prematurely disclose a national security investigation to the target and thereby cause him or her to change his or her behavior patterns to thwart detection;
- B) (U//FOUO) Disclosure may prematurely disclose a national security investigation to other individuals who work with or in some way are affiliated with the target or the subject matter of the national security investigation and thereby cause the other individuals to change their behavior patterns to thwart detection;
- C) (U//FOUO) Disclosure may alert other individuals who use the service of the NSL recipient that the recipient has been asked to provide information to the FBI, and thereby cause the other individuals to change their behavior to thwart detection.
- D) (U//FOUO) Disclosure may persuade those engaged in questionable activities to avoid patronizing the entity known to be subject to requests to reveal account information and thereby allow those persons to thwart detection;
- E) (U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby cause surveillance techniques to be compromised or endanger undercover FBI employees and confidential sources;
- F) (U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby provide an opportunity for someone to create intentionally-flawed (i.e., compromised) foreign intelligence;
- G) (U//FOUO) Disclosure may prematurely disclose a national security investigation involving an hostage situation and thereby endanger the life or safety of a hostage;

- H) (U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby cause the subject or a material witness to flee or to destroy or tamper with evidence;
- I) (U//FOUO) Disclosure may prematurely disclose a national security investigation and thereby result in publicity that makes it difficult for the target of the NSL and/or others to receive a fair trial;
- J) (U//FOUO) Disclosure may prematurely disclose a national security investigation involving an imminent threat of terrorism and thereby endanger the life or safety of others; or
- K) (U//FOUO) Disclosure may reveal the existence of a national security investigation involving a foreign government and thereby damage diplomatic relations.

(U//FOUO) This list is not exhaustive. There may be other reasons why an NSL should not be disclosed, and if so, those reasons should be set forth in the EC.

18.6.6.3.7.2 (U) COPY OF NSL

(U//FOUO) A copy of the signed NSL must be retained in the investigative file and be uploaded under the appropriate NSL document type in ACS. Documented proof of service of NSLs must also be maintained in the NSL sub- file.

18.6.6.3.7.3 (U) SECOND-GENERATION INFORMATION

(U//FOUO) Under limited circumstances, one NSL may simultaneously request toll or transactional information for a “seed number” (normally the target of the investigation) and toll or transactional information for all telephone numbers that have been in contact with the seed number (“second-generation records”). If an NSL seeks second-generation records, the NSL EC must clearly state that second-generation information is being sought and demonstrate the relevance of the second-generation information to the national security investigation. Second-generation phone numbers for which information is obtained must be separately reported to NSLB for Congressional reporting purposes. Requests for second-generation information may only be approved by the DGC of NSLB.

18.6.6.3.7.4 (U) CONTACT WITH MEMBERS OF THE NEWS MEDIA BY A “SEED NUMBER”

(U//FOUO) A second generation NSL may not be used if there is reason to believe the “seed number” has been in contact with members of the news media.

18.6.6.3.7.5 (U) EMERGENCY CIRCUMSTANCES

(U//FOUO) ECPA protects subscriber or communications transactional information from disclosure by providers of telephone or other electronic communication services. Generally, an NSL, grand jury subpoena, or another form of legal process must be used to compel a communication service provider to disclose subscriber or transactional information. In emergency circumstances, however, the provider may voluntarily disclose information to the FBI if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person exists and requires disclosure without delay. As a matter of FBI policy, when there is a danger of death or

serious physical injury that does not permit the proper processing of an NSL, an administrative subpoena (if permissible), a grand jury subpoena, or a letter to the provider citing 18 U.S.C. § 2702 may be used to request emergency disclosure, if approved by a SAC, ASAC, or FBIHQ Section Chief. If time does not permit the issuance of an emergency letter citing 18 U.S.C. § 2702, an oral request to the provider may be made, but the oral request must be followed-up with a letter to the particular provider. In either situation, an FD-1053 Form, which automatically generates the letter, must be completed.

(U//FOUO) The letter (an FD-1053) serves to: (i) obtain the required approval of a SAC or ASAC in a field office or a Section Chief in FBIHQ; and (ii) document the factual basis for the emergency disclosure for inclusion in the investigative file or in a control file (if no investigative file has been opened).

(U//FOUO) This FD-1053 letter should be used instead of any form provided by the provider. If the provider insists that its form must be used in lieu of the standard letter, the provider's form may be used after the form is carefully reviewed and appropriately edited to make clear that: (i) 18 U.S.C. § 2702 authorizes the emergency disclosure; and (ii) subsequent legal process is neither provided nor required by § 2702 and, therefore, no follow-up legal process will be provided. Questions concerning language in the provider's form should be directed to the CDC or OGC/NSLB (national security emergencies) or ILU (criminal law emergencies).

18.6.6.3.8 (U) NOTICE AND REPORTING REQUIREMENTS

(U//FOUO) The National Security Law Branch at FBIHQ compiles NSL statistics for reporting to Congress. The NSL subsystem (FISAMS) automatically records the information needed for Congressional reporting. If the NSL is created outside the subsystem, the EC must include all information necessary for NSLB to report NSL statistics accurately. The EC must delineate the number of targeted phone numbers/e-mail accounts/financial accounts that are addressed to each NSL recipient. For example, if there are three targets, ten accounts, and six recipients of an NSL, the EC must state how many accounts are the subject of the NSL as to Recipient 1, Recipient 2, etc. It is not sufficient to indicate only that there are ten accounts and six recipients.

(U//FOUO) In addition, the FBI must report the USPER status of the subject of all NSLs (as opposed to the target of the investigation), other than NSLs that seek only subscriber information. While the subject is often the target of the investigation, that is not always the case. The EC must reflect the USPER status of the subject of the request – the person whose information the FBI is seeking. If the NSL is seeking information about more than one person, the EC must reflect the USPER status of each person. (See the model ECs on the NSLB website.)

18.6.6.3.9 (U) RECEIPT OF NSL INFORMATION

(U//FOUO) Immediately after receiving material in response to an NSL **and before uploading it into any FBI database**, the employee who initiated the request for the NSL, including an employee of an FBIHQ operational Unit who initiates an NSL in an investigative file that was opened by and resides in a field office, is responsible for ensuring that the

received information is responsive to the request and that there has been no overproduction. If the information is appropriately responsive, the employee who initiated the request for the NSL must ensure that the information is stored in the appropriate investigative file and that receipt of the material is documented in the NSL subsystem. Relevant information properly obtained in response to a valid NSL may be uploaded thereafter into any database. For procedures on how to handle electronic returns from certain ISPs see DIOG Section 18.6.6.3.10.

(U//FOUO) Any material that is not covered within the four corners of the NSL request (including the NSL attachment) must be handled as discussed below. Such information can fall into two categories. First, it can be irrelevant information (hereafter “Irrelevant Information”), which the FBI has no right either to seek or retain. Irrelevant Information is collected, for example, when a telephone company transposes numbers in a telephone number and thereby provides toll billing information concerning the wrong telephone number. Second, it can be relevant information (hereafter “Relevant Overproduction”) but be in excess of what the NSL requested. Relevant Overproduction occurs, for example, when the NSL seeks financial records on John Doe for a specified period. The bank provides the requested records, but the bank also provides records on John Doe beyond the specified period. Both Irrelevant Information and Relevant Overproduction constitute an overproduction, and they must be treated distinctly as described below.

(U//FOUO) Irrelevant Information may not be retained or uploaded into any FBI database. It is therefore critical that all information returned in response to an NSL be reviewed **BEFORE** uploading it into any FBI database, including Telephone Applications. Any Irrelevant Information must either be destroyed or returned to the entity that produced it, at the discretion of the field office or division from which the NSL originated. FBI employees are permitted to destroy the overproduced information, although an SSA must approve the scope of what is to be destroyed. Any Irrelevant Information that is returned electronically and reviewed in Data Warehouse System-ELSUR Data Management System (DWS-EDMS) must be destroyed using the process established in that system. If there is any question whether the information provided is within the scope of the NSL, the CDC or ADC must be consulted.

(U//FOUO) Relevant Overproduction must be sequestered with the employee’s supervisor and may not be uploaded into any FBI database or used in the investigation until another NSL has been served to address the overproduction. The field office or HQ division may serve a “curative” NSL to authorize the retention and use Relevant Overproduction if: (i) the investigation is still pending, (ii) the overproduced information is relevant to the investigation, and (iii) the FBI may lawfully obtain the overproduced information under statutory authority (*i.e.*, an NSL statute). After the “curative” NSL has been served, the FBI may immediately upload and use the sequestered information.

(U//FOUO) If the response contains relevant information within the scope of the NSL, but also contains irrelevant information or relevant overproduction, FBI employees may redact the irrelevant information or the relevant overproduction. The employee’s supervisor must approve the scope of the redaction. If there is any question whether the information provided is within the scope of the NSL, the CDC or OGC must be consulted. The method of redaction is left to the discretion of the employee, but redacted information must not be visible, used in the investigation, or uploaded into any FBI database. The method of redaction will vary

depending on whether the information was provided in hard copy or electronically. After the irrelevant or overproduced information has been redacted, the remainder of properly produced information may be uploaded into any database and used in the investigation.

(U//FOUO) Incidents involving third-party overproduction in response to an NSL where the FBI did not use or upload the overproduced information into any FBI database must be reported to OGC/NSLB for tracking purposes. This type of incident should not be reported as a potential IOB matter. OGC/NSLB will not adjudicate such matters or respond to the report. However, OGC/NSLB uses the information to track third-party NSL overproductions. Procedures for reporting such matters are set forth in sections 4.4 to 4.7 of the Guidance on Intelligence Oversight Board (IOB) Matters, Policy Implementation Guide 0188PG.

(U//FOUO) Incidents involving third-party overproduction in response to an NSL where the FBI used or uploaded the overproduced information into any FBI database must be reported as a potential IOB matter. Procedures for reporting such matters are set forth in sections 4.1 to 4.3 of the Guidance on Intelligence Oversight Board (IOB) Matters, Policy Implementation Guide 0188PG.

(U//FOUO) All responsive records must be placed in an NSL sub-file of the investigative file. These records shall remain with the investigative file until the file is destroyed in accordance with the disposition schedule approved by the National Archives and Records Administration (NARA). The sub-file must be opened in ACS, and the receipt and filing of records must be recorded in an EC.

18.6.6.3.10 (U) ELECTRONIC SERVICE AND ELECTRONIC RETURNS OF NSLS

(U//FOUO) Effective January 31, 2011, absent exigent circumstances or restricted investigations, all NSLs served on certain Internet Service Providers (ISPs) will be served and returns will be received electronically. A current list of ISPs participating in electronic service and electronic returns of NSLs will be maintained on FISAMS.

(U//FOUO) All NSLs will continue to be created in compliance with DIOG Section 18.6.6. The process for service of the NSL will, however, be different. After the NSL has been approved in FISAMS, the employee who initiated the request for the NSL will receive an email notification that DWS-EDMS will deliver the NSL electronically. The field office that issues the NSL must promptly scan the signed NSL and email it to HQ_DIV_18.DITU_NSL. The original NSL must be placed in the appropriate NSL sub-file. Any changes to this process will be posted on DWS-EDMS and FISAMS.

(U//FOUO) NSL returns received electronically will only be available for review in a sequestered area of DWS-EDMS. When the NSL results have been received and loaded into DWS-EDMS, the initiator of the NSL and the case agent will receive notification that the results are available in DWS-EDMS for review for possible overproduced information. If any overproduced information is identified it must be removed from DWS-EDMS. After the employee has confirmed that there is no overproduction, the information may be released into the general DWS-EDMS database for analysis and investigation by any employee who has access to DWS-EDMS. Overproduced return information must be handled pursuant to the directions set forth in DIOG Section 18.6.6.3.9.

(U//FOUO) For NSL returns that are received electronically, the employee who initiated the request for the NSL or his/her designee must upload the electronic results into ACS by:

- A) (U//FOUO) Printing or exporting responsive return information into an Excel spreadsheet, a PDF document, or electronic medium (e.g., CD or DVD) from DWS-EDMS and storing it in the appropriate NSL subfile using a 1A or FD340 envelope which will be reflected in ACS. All hard copy returns from other providers must continue being stored in a 1A or FD340 envelope in the NSL subfile; and
- B) (U//FOUO) Uploading an EC confirming the receipt of the results, including the subject's information, and stating that the results can be located in DWS-EDMS.

(U//FOUO) The employee who initiated the request for the NSL or his/her designee must also ensure that receipt of the records is documented within the NSL subsystem. If the employee wishes, the return information may also be uploaded to ACS or other databases.

(U//FOUO) More information about DWS-EDMS, including its review and analytic tools, easy access links, and a step-by-step guide to requesting access can be obtained at the STAO web page (<http://home.fbinet.fbi/STB/stao/STAOOPS/ATAU/Pages/DWS-EDMS.aspx>).

(U//FOUO) Any employee who may need access to NSL data received electronically (either for analytic or investigative purposes or to review for overproduction) must obtain access to DWS-EDMS. Instructions and requirements for gaining access to DWS-EDMS can be found on the STAO web page noted above.

18.6.6.3.11 (U) DISSEMINATION OF NSL MATERIAL

(U//FOUO) Subject to certain statutory limitations, information obtained in response to an NSL may be disseminated according to general dissemination standards in the AGG-Dom. The ECPA (telephone and electronic communications transactional records) and RFPA (financial records) permit dissemination if consistent with the AGG-Dom and the information is clearly relevant to the responsibilities of the recipient agency. FCRA permits dissemination of identity of financial institutions and consumer identifying information to other federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation. FCRA imposes no special rules for dissemination of full credit reports.

(U//FOUO) Although the requesting EC is generally classified because it reflects the predicate for the investigation and the need for the NSL, NSLs are not classified nor is the material received in return classified. Information obtained in response to an NSL may be used in criminal proceedings without any declassification. In addition, information provided in response to an NSL that was obtained with an e-mail, telephone or other account number learned through FISA coverage is not considered FISA-derived and, therefore, approval from the Attorney General to use such information is not required.

18.6.6.3.12 (U) SPECIAL PROCEDURES FOR HANDLING RIGHT TO FINANCIAL PRIVACY ACT INFORMATION

(U//FOUO) For financial records received in response to a RFPA NSL, the employee who initiated the NSL or his/her designee must review the various items contained within the records (e.g., checks written, items deposited, credit card charges) and determine whether the

information holds current or potential investigative value (i.e., whether it provides a new investigative need, addresses an existing investigative need, contributes to an existing intelligence collection requirement, or serves some other lawful investigative purpose that has arisen since the NSL was issued) or has the reasonable potential to provide other FBI or Intelligence Community employees information of value consistent with their mission. Information that is determined not to have current investigative value but that is responsive to the NSL may be retained in the hardcopy investigative file but may not be uploaded into ACS or other electronic databases.

(U//FOUO) Only items that have current or potential investigative value should be included in products uploaded into ACS. Typically, such information is uploaded into ACS by way of an Excel spreadsheet or a summary of items by category (e.g., wire transfers or deposit items) included in an EC. An employee should upload the EC containing the summary of the records in an NSL sub-file in the electronic case management system so that such records may be later identified and easily retrieved.

(U//FOUO) There is no requirement for determining the investigative value regarding responsive information provided in response to a FCRA or an ECPA NSL because such information will always have investigative value or it is necessary to upload and engage in cross-correlations to ascertain value that may not be obvious.

(U//FOUO) For additional information regarding the handling of information provided in response to an NSL, see the Attorney General approved Procedures for the Collection, Use, and Storage of Information Derived from National Security Letters.

18.6.6.3.13 (U) PAYMENT FOR NSL-DERIVED INFORMATION

(U//FOUO) No legal obligation exists for the FBI to compensate recipients of NSLs issued pursuant to ECPA (telephone and electronic communications transactional records) or FCRA, 15 U.S.C. § 1681v (full credit reports in international terrorism investigations), and therefore no payment should be made in connection with those NSLs. See EC, 319X-HQ-A1487720-OGC, serial 222, for a form letter to be sent in response to demands for payment concerning these NSLs.

(U//FOUO) Compensation is legally required for NSLs issued pursuant to RFPA (financial records) and FCRA § 1681u (identity of financial institutions and consumer identifying information). A fee schedule has been adopted under 12 C.F.R. § 219.3, Appendix A, and should be reviewed for the current reimbursement provisions. A copy of this fee schedule is available on the OGC website at:
http://home.fbinet.fbi/DO/OGC/Main%20Law%20Library/cost_reimbursement_guidance.pdf

18.6.7 (U) INVESTIGATIVE METHOD: FISA ORDER FOR BUSINESS RECORDS (COMPULSORY PROCESS)

18.6.7.1 (U) OVERVIEW OF COMPULSORY PROCESS

(U//FOUO) Compulsory processes may be used to compel the disclosure of any tangible things (including books, records, papers, documents and other items) relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Compulsory process in a Predicated Investigation includes, but is not limited to, the use of FISA business records orders (described below in this section); administrative subpoenas (DIOG Section 18.6.4); grand jury subpoenas (DIOG Sections 18.6.5 and 18.5.9); trial subpoenas requested by the prosecuting attorney and issued by the trial judge; and NSL (DIOG Section 18.6.6). Compulsory process is used to gather information in furtherance of FBI investigations. The FBI's authority to use such compulsory process is based upon Executive Branch delegated authorizations, statutes, regulations and the FRCP.

(U) An FBI CHS cannot be tasked to obtain records protected by the RFP, FCRA, ECPA, Buckley Amendment, except as specifically authorized by such law.

18.6.7.2 (U) APPLICATION

(U//FOUO) FISA Business Records Orders may be used during authorized national security investigations. This method may not be used for assistance to other agencies, unless relevant to an already open FBI authorized investigation. When collecting positive foreign intelligence, if the subject is a non-USPER, a request for business records pursuant to 50 U.S.C. §§ 1861-63 is lawful. This method may not be used in an Assessment.

18.6.7.3 (U) BUSINESS RECORDS UNDER FISA

18.6.7.3.1 (U) LEGAL AUTHORITY

(U) 50 U.S.C. §§ 1861-63

18.6.7.3.2 (U) DEFINITION OF METHOD

(U) A FISA order for business records, is an order for a third party to produce documents, records, and other tangible things (including books, records, papers, documents, and other items) relevant to an authorized national security investigation. A FISA order for business records may not be obtained during an Assessment. FISA business records orders may not be used to obtain information during a positive foreign intelligence investigation if the material sought relates to an USPER.

The FBI and DOJ are addressing the issue of whether the Attorney General must approve any use of information obtained or derived from a FISA business records order in any criminal, civil, immigration, military, or other proceeding, including any proceeding outside the United States. (Although there is no statutory requirement to obtain Attorney General authorization, the FBI and DOJ are working to determine whether, by policy, such authorization is required.) Until that issue is addressed, FBI employees must consult with their CDC or an NSLB attorney to determine whether advanced authorization of the Attorney General must be obtained.

18.6.7.3.3 (U) APPROVAL REQUIREMENTS

(U//FOUO) All requests for FISA business records orders must be submitted through FISAMS to NSLB, which will draft the application. The request and the draft application must then be submitted to the DOJ Office of Intelligence (OI). Each request must include a statement of the facts and circumstances relied upon by the applicant to establish that the records sought are relevant to an authorized investigation, and supporting the need for non-disclosure, if non-disclosure is requested. Requests classified up to Secret must be submitted through FISAMS on FBINET. Requests classified Top Secret (TS) and/or Special Compartmentalized Information (SCI) must be submitted through FISAMS on SCION. Field offices not having SCION access must prepare a paper copy of the request form, route it for appropriate signatures, and thereafter secure fax the request form to the FBIHQ operational unit handling the request. The operational unit will enter the request into FISAMS on SCION. In field offices not having SCION access, the SAC, CDC, and ASAC must sign the paper copy of TS and/or SCI requests.

(U//FOUO) The Director has delegated the authority to make an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, only to the Deputy Director and the Executive Assistant Director for National Security.

18.6.7.3.4 (U) DURATION OF COURT APPROVAL

(U) Authority for a FISA business records order is established by court order.

18.6.7.3.5 (U) NOTICE AND REPORTING REQUIREMENTS

(U) There are no special notice or reporting requirements.

18.6.7.3.6 (U) COMPLIANCE REQUIREMENTS

(U) The employee who receives material produced in response to a FISA business records order must do the following:

- A) (U//FOUO) Handle the material as required by the Standard Minimization Procedures Adopted for Business Records Orders and any specialized minimization procedures required by the Foreign Intelligence Surveillance Court (FISC) in connection with the particular order for production.
- B) (U) See the current classified FISA Business Records standard minimization procedures: http://home.fbinet.fbi/DO/OGC/NSLB/Documents/business_records_minimization_procedure_s.pdf.

18.6.7.3.7 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization ("FISA overcollection") will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.6.8 (U) INVESTIGATIVE METHOD: STORED WIRE OR ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS

18.6.8.1 (U) SUMMARY

(U//FOUO) FBI employees may acquire the contents of stored wire or electronic communications and associated transactional records—including basic subscriber information—as provided in 18 U.S.C. §§ 2701-2712 (Electronic Communications Privacy Act (ECPA)). Requests for voluntary disclosure under the emergency authority of 18 U.S.C. § 2702 require prior approval from the field office ASAC or FBIHQ Section Chief when appropriate.

(U//FOUO) All requests for information from electronic communication service providers (e.g., telephone companies, internet service providers) pertaining to a subscriber or customer must comply with ECPA. As used in ECPA, the term “information pertaining to a subscriber or customer” should be read broadly. It includes, for example, information regarding whether a particular individual has an account with a covered provider. Thus, unless done in accordance with ECPA, an FBI employee may not ask a telephone company or internet service provider whether John Smith has an account with the company (i.e., the FBI employee may not informally seek information that is statutorily protected prior to the issuance of appropriate process or the existence of an exception to ECPA). In addition, based on a November 5, 2008 interpretation of ECPA from the Office of Legal Counsel, the FBI may not ask a telephone company whether a given telephone number that the company services has been assigned to an individual. In short, in order to obtain any information specific to the subscriber from a telephone company or electronic communication service provider, the FBI must provide legal process pursuant to 18 U.S.C. §§ 2703 or 2709 or the request must fall within the limited exceptions established in 18 U.S.C. § 2702, and discussed below.

(U//FOUO) ECPA does not, however, protect information that is not tied to a particular subscriber. Thus, the FBI does not need legal process or an exception to ECPA to ask a telephone company whether it services a particular telephone number or to obtain blocks of telephone numbers that are serviced by the particular company.

18.6.8.2 (U) APPLICATION

(U//FOUO) This investigative method may be used during national security Predicated Investigations and criminal Predicated Investigations as authorized by statute. The use of Search Warrants to obtain this information in Preliminary Investigations is prohibited. (See DIOG Section 18.6.8.4.2.3 below) This method may not be used for assistance to other agencies, unless the information to be obtained is relevant to an already open Predicated Investigation. This method cannot be used to collect positive foreign intelligence or during an Assessment.

18.6.8.2.1 (U) STORED DATA

(U) The Electronic Communications Privacy Act (ECPA)—18 U.S.C. §§ 2701-2712—governs the disclosure of two broad categories of information: (i) the contents of wire or

electronic communications held in “electronic storage” by providers of “electronic communication service” or contents held by those who provide “remote computing service” to the public; and (ii) records or other information pertaining to a subscriber to or customer of such services. The category of “records or other information” can be subdivided further into subscriber records (listed in 18 U.S.C. § 2703(c)(2)) and stored traffic data or other records.

(U) Records covered by ECPA include all records that are related to the subscriber, including buddy lists, “friend” lists (MySpace), and virtual property owned (Second Life). These other sorts of records are not subscriber records and cannot be obtained with a subpoena under 18 U.S.C. § 2703(c)(2) or an NSL under 18 U.S.C. § 2709.

18.6.8.2.2 (U) LEGAL PROCESS

(U) The legal process for obtaining disclosure will vary depending on the type of information sought and whether the information is being voluntarily provided under 18 U.S.C. § 2702 (e.g., with consent or when emergency circumstances require disclosure) or the provider is being compelled to provide the information under 18 U.S.C. § 2703, as outlined below. The process for compelling production under 18 U.S.C. § 2709 is discussed in the NSL section above.

18.6.8.2.3 (U) RETRIEVAL

(U) Contents held in “electronic storage” by a provider of “electronic communication service” for 180 days or less can only be obtained with a search warrant based on probable cause. Accordingly, such records may only be obtained during a Full Investigation.

(U) Contents held by those who provide “remote computing service” to the public and contents held in “electronic storage” for more than 180 days by an “electronic communication service” provider can be obtained with: a warrant; a subpoena with prior notice to the subscriber or customer; or an order issued by a court under 18 U.S.C. § 2703(d) when prior notice has been provided to the customer or subscriber (unless the court has authorized delayed notice).

(U) Title 18 U.S.C. § 2705 establishes the standard to delay notice for an initial period of up to 90 days. Records or other information pertaining to a subscriber to or customer of such services, including basic subscriber information, can be obtained with a search warrant or an 18 U.S.C. § 2703(d) order without notice.

18.6.8.2.4 (U) BASIC SUBSCRIBER INFORMATION

(U) Basic subscriber information, as described in 18 U.S.C. § 2703(c)(2), can be compelled by a grand jury or administrative subpoena without notice.

18.6.8.2.5 (U) PRESERVATION OF STORED DATA

(U) The government is authorized under 18 U.S.C. § 2703(f) to direct a provider to preserve records or other information (stored records or communications) in its possession for 90 days (which may be extended for an additional 90-days) pending issuance of applicable legal

process for disclosure. To make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process.

18.6.8.2.6 (U) COST REIMBURSEMENT

(U) 18 U.S.C. § 2706 requires the government to reimburse for costs incurred in providing the contents of communications, records, or other information obtained under 18 U.S.C. §§ 2702, 2703, or 2704, except that reimbursement is not required for records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under 18 U.S.C. § 2703. In essence, the government does not have to reimburse for the cost of producing records that the provider maintains in the ordinary course of its business.

18.6.8.3 (U) LEGAL AUTHORITY

(U) 18 U.S.C. §§ 2701-2712

(U) AGG-Dom, Part V.9

(U) ECPA—18 U.S.C. §§ 2701-2712—creates statutory privacy rights for the contents of communications in “electronic storage” and records or other information pertaining to a subscriber to or customer of an “electronic communication service” and a “remote computing service.” The statutory protections protect the privacy of an individual’s electronic data contained in a networked account—that may otherwise fall outside the scope of the protections afforded by the Fourth Amendment—when such account or its service is owned or managed by a third-party provider.

(U) ECPA generally: (i) prohibits access to the contents of wire or electronic communications while in “electronic storage” unless authorized (18 U.S.C. § 2701); (ii) prohibits a provider of service to the public from disclosing the contents of wire or electronic communications while held in “electronic storage,” and prohibits divulging to the government any information pertaining to a subscriber to or customer of such service unless authorized (18 U.S.C. § 2702); and (iii) authorizes the government to compel disclosure from a provider of stored contents of a wire or electronic communication and records or other information pertaining to a subscriber to or customer (18 U.S.C. § 2703). ECPA provides for reimbursement of costs incurred in providing the information acquired.

(U) An FBI CHS cannot be tasked to obtain records protected by ECPA except as specifically authorized by such law.

18.6.8.4 (U) ECPA DISCLOSURES

(U) ECPA authorities can be divided into two categories: (i) compelled disclosure—legal process to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail—opened and unopened) and other information, such as account records and basic subscriber information; and (ii) voluntary disclosure of such information from service providers. Each of these authorities is discussed below.

18.6.8.4.1 (U) DEFINITIONS

- A) (U) **Electronic Storage**: is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," or "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). In short, "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.
- B) (U) **Remote Computing Service (RCS)**: is a service that provides "to the public" computer storage or processing services by means of an electronic communications system. 18 U.S.C. § 2711(2). In essence, a remote computing service is an off-site computer that stores or processes data for a customer.
- C) (U) **Electronic Communications System**: is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).
- D) (U) **Electronic Communication Service (ECS)**: is "any service that provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

18.6.8.4.2 (U) COMPELLED DISCLOSURE

(U) 18 U.S.C. § 2703 lists five types of legal process that the government can use to compel a provider to disclose certain kinds of information. The five mechanisms, in descending order of required threshold showing are as follows:

- A) (U) Search warrant;
- B) (U) 18 U.S.C. § 2703(d) court order with prior notice to the subscriber or customer;
- C) (U) 18 U.S.C. § 2703(d) court order without prior notice to the subscriber or customer;
- D) (U) Subpoena with prior notice to the subscriber or customer; and
- E) (U) Subpoena without prior notice to the subscriber or customer.

(U) Generally, anything that can be obtained under ECPA with greater process includes access to information that can be obtained with lesser process. Thus, a search warrant can compel the production of everything that an 18 U.S.C. § 2703(d) order can compel (and then some), and an 18 U.S.C. § 2703(d) court order can compel everything that a subpoena can compel (plus additional information). The notice requirement, however, must be considered as a separate burden under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using an 18 U.S.C. § 2703(d) order without subscriber notice.

(U) **Note for Telemarketing Fraud**: When investigating telemarketing fraud, law enforcement may make a written request to the service provider to obtain the name, address, and place of business of a subscriber or customer engaged in telemarketing. See 18 U.S.C. § 2703(c)(1)(D). These requests do not require notice to the customer.

18.6.8.4.2.1 (U//FOUO) NOTICE—ORDERS NOT TO DISCLOSE THE EXISTENCE OF A WARRANT, SUBPOENA, OR COURT ORDER

(U//FOUO) FBI employees may obtain a court order directing network service providers not to disclose the existence of compelled process if the government has no legal duty to notify the customer or subscriber of the process. If an 18 U.S.C. § 2703(d) order or 18 U.S.C. § 2703(a) warrant is being used, a request for a non-disclosure order can be included in the application and proposed order or warrant. If a subpoena is being used to obtain the information, a separate application to a court for a non-disclosure order must be made.

18.6.8.4.2.2 (U) LEGAL STANDARD

(U//FOUO) A court may order an electronic communications service provider or remote computing service not to disclose the existence of a warrant, subpoena, or court order for such period as the court deems appropriate. The court must enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:

- A) (U) Endangering the life or physical safety of an individual;
- B) (U) Flight from prosecution;
- C) (U) Destruction of or tampering with evidence;
- D) (U) Intimidation of potential witnesses; or
- E) (U) Otherwise seriously jeopardizing an investigation or unduly delaying a trial. 18 U.S.C. § 2705(b).

18.6.8.4.2.3 (U) SEARCH WARRANT

(U//FOUO) Investigators can obtain the full contents of a network account with a search warrant issued pursuant to FRCP Rule 41. However, FRCP Rule 41 search warrant may not be issued in Preliminary Investigations. See DIOG Section 18.7.1.3.4.4.

18.6.8.4.2.4 (U) COURT ORDER WITH PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//FOUO) Investigators can obtain everything in a network account except for unopened e-mail or voice-mail stored with a provider for 180 days or less using a 18 U.S.C. § 2703(d) court order with prior notice to the subscriber unless they have obtained authority for delayed notice pursuant to 18 U.S.C. § 2705. ECPA distinguishes between the contents of communications that are in "electronic storage" (e.g., unopened e-mail) for less than 180 days, and those that have been in "electronic storage" for longer or that are no longer in "electronic storage" (e.g., opened e-mail).

(U) FBI employees who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a), may obtain:

A) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

B) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703 (b)(2); and

C) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order without notice.

(U) As a practical matter, this means that the government can obtain all associated subscriber and transactional records and the full contents of a subscriber's account except unopened e-mail and voicemail (that has been in "electronic storage" 180 days or less) using a 18 U.S.C. § 2703(d) order that complies with the prior notice provisions of 18 U.S.C. § 2703(b)(1)(B).

(U) If notice would jeopardize the investigation, FBI employees can obtain an order delaying notice for up to ninety days. See 18 U.S.C. § 2705(a). A request to delay notice may be included in the 18 U.S.C. § 2703(d) application and proposed order. FBI employees may also apply to the court for extensions of the delay. See 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(4). Upon expiration of the delayed notice period, the government is required to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5).

18.6.8.4.2.4.1 (U) LEGAL STANDARD

(U) To order delayed notice, the court must find that "there is reason to believe that notification of the existence of the court order may... endanger the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew each time an extension of the delayed notice is sought.

18.6.8.4.2.4.2 (U) NATIONWIDE SCOPE

(U) Federal court orders under 18 U.S.C. § 2703(d) have effect outside the district of the issuing court. Orders issued pursuant to 18 U.S.C. § 2703(d) may compel providers to disclose information even if the information is stored outside the district of the issuing court. See 18 U.S.C. § 2703(d) ("any court that is a court of competent jurisdiction" may issue a 18 U.S.C. § 2703(d) order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

(U) 18 U.S.C. § 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B). These orders issued by state courts, however, do not have effect outside the jurisdiction of the issuing state. See 18 U.S.C. §§ 2711(3).

18.6.8.4.2.5 (U) COURT ORDER WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U) A court order under 18 U.S.C. § 2703(d) may compel disclosure of:

A) (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and

B) (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1).

18.6.8.4.2.5.1 (U) TYPES OF TRANSACTIONAL RECORDS

(U) The broad category of transactional records includes all records held by a service provider that pertain to the subscriber beyond the specific records listed in 2703(c)(2) such as a list of "friends" as used in social networking sites and virtual property owned as used in virtual worlds.

(U//FOUO) Non-content cellular location information falls into one of two general categories: (i) cell site and sector information; or (ii) other provider-assisted geo-location information. FBI employees must contact the CDC and/or the AUSA assigned to the investigation to determine what legal process may be required as court decisions in the federal districts and circuits vary on this issue.

18.6.8.4.2.5.2 (U) CELL SITE AND SECTOR INFORMATION

(U) Cell site and sector information is considered "a record or other information pertaining to a subscriber" and therefore, production of historical and prospective cell site and sector information may be compelled by a court order under 18 U.S.C. § 2703(d). Requests made pursuant to 18 U.S.C. § 2703(d) for disclosure of prospective cell site and sector information—which is delivered to law enforcement under Communications Assistance for Law Enforcement Act (CALEA) at the beginning and end of calls—must be combined with an application for pen register/trap and trace device. Some judicial districts will require a showing of probable cause before authorizing the disclosure of prospective cell site and sector information.

18.6.8.4.2.5.3 (U) OTHER GEO-LOCATION INFORMATION AVAILABLE TO THE PROVIDER

(U) Geo-location data that is distinct from cell site (tower/sector) data has been developed by carriers, in part, to deliver certain location data for 911 calls and is implemented either through network-based or handset-based means. It is important to note that only some of the cellular providers currently have the capability to make this data available to law enforcement. Each of these location methods differs materially from the tower/sector information that is used by the provider's network in the normal provisioning of service and that CALEA requires the provider to be able to deliver to law enforcement. Handset-based methods typically involve the use of GPS technology in which the data resides on the phone itself. Network-based methods measure the radio

frequency signals that are being transmitted from the user's phone handset during registration and/or call processing to at least one tower receiving the signal.

(U//FOUO) In the ordinary course of providing service to the customer, the provider does not typically use this GPS location data. Accordingly, the data may not constitute a "record or other information" in the provider's custody within the meaning of 18 U.S.C. §§ 2702 and 2703. Consequently, a FRCP Rule 41 search warrant should be obtained to compel the disclosure of such provider-assisted geo-location data. The order should: (i) be obtained in the district where the phone is located (as determined by tower data, visual surveillance, or CHS reporting); (2) seek permission to execute outside of daytime hours; (3) request disclosure for no longer than 30 days; and (4) request delayed notice under 18 U.S.C. § 3103a(b) for 30 days with notice ultimately given to the customer or subscriber. The return should note "the exact date and time the device was installed and the period during which it was used"—i.e., it should conform to the FRCP Rule 41 tracking device rule (which does not, by its terms, apply but which is analogous), and the return should be made within 10 calendar days after use ends.

(U) Recognized exceptions to the warrant requirement may, however, apply in certain situations. For example, if cellular geo-location data is requested from a provider in an "exigent circumstance" based on an objectively reasonable basis to believe that the requested information is relevant to an emergency involving danger of death or serious physical injury, such disclosure would arguably be permissible either under 18 U.S.C. § 2702(c)(4)—to the extent ECPA applies—or under the exigent circumstances exception to the warrant requirement (if a warrant were required).

(U) This standard only applies to stored information. For prospective information, DOJ recommends an emergency PR/TT order and an 18 U.S.C. § 2703(d) order should also be obtained when judicial approval is sought according to the PR/TT statute.

18.6.8.4.2.5.4 (U) LEGAL STANDARD

(U) A court order under 18 U.S.C. § 2703(d) is known as an "articulable facts" court order or simply a "d" order. This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant.

(U) In applying for an order pursuant to 18 U.S.C. § 2703 (d), the FBI must state sufficient specific and articulable facts for the court to find that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this standard.

18.6.8.4.2.6 (U) SUBPOENA WITH PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//FOUO) Investigators can subpoena opened e-mail from a provider if they give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. §

2705(a)—which requires a written certification by the SAC or ASAC that there is reason to believe notification of the existence of the subpoena may have an adverse result.

(U) FBI employees who obtain a subpoena and give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a) may obtain:

- A) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2);
- B) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and
- C) (U) Basic subscriber information listed in 18 U.S.C. § 2703(c)(2).

(U) As a practical matter, this means that FBI employees can obtain opened e-mail (and other "unopened" stored wire or electronic communications in "electronic storage" more than 180 days) using a subpoena, so long as they provide prior notice to the subscriber or comply with the delayed notice provisions.

(U) **Notice:** Prior notice of the subpoena must be provided unless a supervisory official has certified in writing that there is reason to believe that notification of the existence of the subpoena may have an adverse result, 18 U.S.C. § 2705(a)(1)(B) and 18 U.S.C. § 2705(a)(4) (authorizing 90-day extensions), in which case notice may be delayed for up to 90 days. The term "supervisory official" is defined to mean the SAC or ASAC or an equivalent level official at headquarters. 18 U.S.C. § 2705(a)(6). Upon expiration of the *delayed notice period*, the government is required to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5). This documentation must be placed with the subpoena in the appropriate investigative file.

(U) **Legal standards for delaying notice:** The supervisory official must certify in writing that "there is reason to believe that notification of the existence of the court order may... endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or... otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). This standard must be satisfied anew every time an extension of the delayed notice is sought. This documentation must be placed with the subpoena in the appropriate investigative file.

18.6.8.4.2.7 (U) SUBPOENA WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//FOUO) Without notice to the subscriber or customer, investigators can subpoena basic subscriber information:

(U) name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service used; telephone or instrument number or other subscriber number or identity, including

any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)[.]" 18 U.S.C. § 2703(c)(2).

(U) These items typically relate to the identity of a subscriber, his or her relationship with the service provider, and basic session connection records. This list does not include other, more extensive transaction-related records, such as logging information revealing the e-mail addresses of persons with whom a customer corresponded during a prior session. In the Internet context, "records of session times and durations," as well as "any temporarily assigned network address" include the IP address assigned by an Internet service provider to a customer for a particular session. They also include other information relating to account access, such as the originating telephone number for dial-up Internet access or the IP address of a user accessing an account over the Internet. See PATRIOT Act § 210, 115 Stat. 272, 283 (2001).

A) (U) **Legal Standard:** The legal threshold for issuing a subpoena is relevance to the investigation. Courts are reluctant to review the "good faith" issuance of subpoenas as long as they satisfy the following factors¹⁷: (i) the investigation is conducted pursuant to a legitimate purpose; (ii) the information requested under the subpoena is relevant to that purpose; (iii) the agency does not already have the information it is seeking with the subpoena; and (iv) the agency has followed the necessary administrative steps in issuing the subpoena.

(U//FOUO) In the event that a federal grand jury subpoena is used, however, appropriate protections against disclosure must be followed in compliance with FRCP Rule 6(e).

B) (U//FOUO) **Fugitive Investigations:** It is a misuse of the grand jury to use the grand jury as an investigative aid in the search for a fugitive in whose testimony the grand jury has no interest. Therefore, grand jury subpoenas for telephone billing records should not be requested in federal fugitive investigations. (See DIOG Section 18.6.5.1 for limited situations in which courts have recognized when grand jury efforts to locate a fugitive are proper.)

C) (U) **Members of the News Media:** Approval of the Attorney general must be obtained prior to seeking telephone billing records of a member of the news media. (See DIOG Section 18.6.5.1.5)

18.6.8.4.3 (U) VOLUNTARY DISCLOSURE

(U) In order to determine whether a provider of an Electronic Communication Service (ECS) or a Remote Computing Service (RCS) can voluntarily disclose contents or records, it must first be determined whether the relevant service is offered by the provider to the public.

A) (U) **Service NOT Available to the Public:** ECPA does not apply to providers of services that are not available "to the public;" accordingly such providers may freely disclose both contents and other records relating to stored communications. *Andersen Consulting v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998) (giving hired consulting firm employees access to UOP's e-mail system is not equivalent to providing e-mail to the public).

B) (U) **Services That ARE Available to the Public:** If the provider offers services to the public, then ECPA governs the disclosure of contents and other records.

¹⁷ (U) *United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950).

- C) (U) If the provider is authorized to disclose the information to the government under 18 U.S.C. § 2702 and is willing to do so voluntarily, law enforcement does not need to obtain a legal order or provide other legal process to compel the disclosure.
- D) (U) If a provider voluntarily discloses under the statute, there is no follow-up legal process required or available. If the provider, on the other hand, either may not or will not disclose the information voluntarily, FBI employees must rely on compelled disclosure provisions and obtain the appropriate legal orders.
- 1) (U) **Voluntary Disclosure of Stored Contents** - ECPA authorizes the voluntary disclosure of stored contents when:
- a) (U) The originator, addressee, intended recipient, or the subscriber (in the case of opened e-mail) expressly or impliedly consents, 18 U.S.C. § 2702(b)(3);
 - b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(b)(5);
 - c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(b)(8);
 - d) (U//FOUO) An emergency disclosure under this statutory exception is justified when the circumstances demand action without delay to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example, an e-mail that discusses a planned terrorist attack but not the timing of the attack would constitute an emergency that threatens life or limb and requires action without delay, even though the timing of the attack is unknown. It is the need for action without delay to prevent the serious harm threatened rather than the immediacy of the threat itself that provides the justification for voluntary disclosures under this exception. H.R. Rep. No. 107-497 at 13-14 (2002) accompanying The Cyber Security Enhancement Act of 2002, H.R. 3482, which passed as part of the comprehensive Homeland Security Act of 2002, Pub. L. No. 107-296, § 225 116 Stat. 2135 (2002).
 - e) (U) The disclosure is made to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990, (42 U.S.C. § 13032 and 18 U.S.C. § 2702[b](6)); or
 - f) (U) The contents are inadvertently obtained by the service provider and appear to pertain to the commission of a crime. Such disclosures can only be made to a law enforcement agency. 18 U.S.C. § 2702(b)(7)
- 2) (U) **Voluntary Disclosure of Non-Content Customer Records** - ECPA permits a provider to voluntarily disclose non-content customer records to the government when:
- a) (U) The customer or subscriber expressly or impliedly consents, 18 U.S.C. § 2702(c)(2);
 - b) (U) The disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(c)(3);
 - c) (U) The provider "in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," 18 U.S.C. § 2702(c)(4); or

- d) (U//FOUO) *Note:* An emergency disclosure under this statutory exception is justified when the circumstances demand immediate action (i.e., obtaining/disclosing information "without delay") to prevent death or serious bodily injury; the statute does not depend on the immediacy of the risk of danger itself. For example, an e-mail that discusses a planned terrorist attack but not the timing of the attack would constitute an emergency that threatens life or limb and requires immediate action, even though the timing of the attack is unknown. It is the need for immediate action to prevent the serious harm threatened rather than the immediacy of the threat itself that provides the justification for voluntary disclosures under this exception. H.R. Rep. No. 107-497 at 13-14 (2002) accompanying The Cyber Security Enhancement Act of 2002, H.R. 3482, which passed as part of the comprehensive Homeland Security Act of 2002, Pub. L. No. 107-296, § 225 116 Stat. 2135 (2002).
- e) (U) The disclosure is to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under Section 227 of the Victims of Child Abuse Act of 1990. (42 U.S.C. § 13032 and 18 U.S.C. § 2702[c][5])
- 3) (U) **Preservation of Evidence under 18 U.S.C. § 2703(f)** - FBI employees may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests, however, have no prospective effect.
- a) (U) Because there is generally no law regulating how long a network service provider must retain account records, there is a risk that evidence might be destroyed or lost in the normal course of the provider's business before law enforcement can obtain legal process to compel disclosure. A governmental entity is authorized to direct providers to preserve stored records and communications pursuant to 18 U.S.C. § 2703(f). Once a preservation request is made, ECPA requires that the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703 (f)(2).
- b) (U) There is no legally prescribed format for 18 U.S.C. § 2703(f) requests. While a phone call should be adequate, a facsimile or an e-mail is better practice because it both provides a paper record and guards against miscommunication.
- c) (U) FBI employees who send 18 U.S.C. § 2703(f) letters to network service providers should be aware of two limitations. First, the authority to direct providers to preserve records and other evidence is not prospective. Thus, 18 U.S.C. § 2703(f) letters can order a provider to preserve records that have already been created but cannot order providers to preserve records not yet made. If FBI employees want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes. A second limitation of 18 U.S.C. § 2703(f) is that some providers may be unable to comply effectively with 18 U.S.C. § 2703(f) requests without having an unintended adverse impact on the investigation. Effective communication with the provider about the practical impact and limitations of implementing the preservation request will enable the FBI employee to make an informed decision regarding preservation.
- 4) (U) **Video Tape Rental or Sales Records** - 18 U.S.C. § 2710 makes the unauthorized disclosure of records by any person engaged in the rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials unlawful and provides an exclusionary rule to prohibit personally identifiable information otherwise obtained from being admissible as evidence in any court proceeding. Personally identifiable information is defined as "information that identifies a person as having requested or obtained specific video material or services"

- a) (U) The disclosure to law enforcement of “personally identifiable information” is permitted only when the law enforcement agency:
 - (i) (U) Has the written consent of the customer;
 - (ii) (U) Obtains a search warrant issued under Rule 41, FRCP or equivalent state warrant; or
 - (iii) (U) Serves a grand jury subpoena;
- b) (U) The disclosure to law enforcement of the name and address of a customer of a video tape service provider may be made without compulsory process when: the information being sought does not identify the customer as having requested or obtained specific video materials or service, and if the customer had prior opportunity to prohibit such disclosure.
- c) (U) This type of information was specifically not included in the definition of “personally identifiable information” to allow law enforcement to obtain information about individuals during routine investigations such as neighborhood investigations.
- d) (U//FOUO) The disclosure of “personally identifiable information” in a national security investigation may be compelled through use of the above legal processes or pursuant to a business records order issued under 50 U.S.C. § 1861.

18.6.8.5 (U) VOLUNTARY EMERGENCY DISCLOSURE

18.6.8.5.1 (U) SCOPE

(U//FOUO) ECPA protects subscriber and transactional information regarding communications from disclosure by providers of remote computing services or telephone or other electronic communication services to the public (remote computing services, telephone and other electronic communications services are hereafter collectively referred to as “electronic communications service providers” or “providers”). Generally, an NSL, grand jury subpoena, or other form of legal process must be used to compel the communication service provider to disclose such information. Pursuant to 18 U.S.C. § 2702, however, an electronic communications service provider may voluntarily disclose customer records or the stored contents of communications to the FBI if the service provider believes in good faith that an emergency exists involving danger of death or serious physical injury to any person which requires disclosure of such information without delay. The information necessary to satisfy the emergency disclosure standard may be provided by the FBI or may arise from information the electronic communications service provider independently acquires. No matter how the information is acquired, the statutory provision does not provide authority for the FBI to compel disclosure from the provider. Nor does the statute require any follow up legal process (e.g., a subpoena or NSL, etc.) if an emergency disclosure is made.

(U//FOUO) The FD-1053 **must** be used when requesting emergency voluntary disclosures from an electronic communications service provider. The form will automatically generate a letter which must be signed and furnished to the provider. If time does not permit the issuance of an emergency letter, an oral request may be made, but the oral request must be followed-up with a request letter. The request letter informs the provider that further legal process is not required and will not be forthcoming.

(U//FOUO) The FD-1053 must also be used in those circumstances when the electronic communications service provider voluntarily discloses such information without a request from the FBI. In these circumstances, the FD-1053 will not generate a request letter, but it will facilitate other required record keeping, as discussed below.

(U//FOUO) In either situation, the FD-1053 (and a copy of the signed request letter, if one is generated and provided to the electronic communications service provider) must be serialized in the investigative file, including the hardcopy file.

(U//FOUO) The use of the FD-1053 form is designed to capture all the information the FBI needs to satisfy statutory annual Congressional reporting requirements.

(U//FOUO) If the employee provides the FD-1053 letter to an electronic communications service provider and the provider instead insists that the employee use the provider's standard form letter, the employee should contact his/her CDC or OGC immediately; often times, the provider's forms contain language representing that some type of legal process will be furnished subsequently. In such situations, if obtaining CDC or OGC guidance is not feasible under the emergency circumstances, the employee must strike out any language referencing future legal process (e.g., NSL or subpoena) from the provider's standard form and hand-write on the provider's standard form language that makes clear the information is being provided voluntarily pursuant to the ECPA and that legal process will not be provided. With such edits (if necessary) the provider's revised form may be used and a copy must be maintained in the investigative file. If the electronic communications service provider will not permit such a change to its standardized letter, the provider's letter may be used. The employee must document in an EC to the investigative file, as soon as practicable but no later than five (5) business days after the emergency disclosure is made, the name, title, and contact information of the provider's employee who refused to modify the letter and such employee's reason for refusing to accept the FD-1053. A copy of the EC must be sent to the CDC and the Deputy General Counsel of the National Security Law Branch or the Investigative Law Branch as determined by the type of investigation. The employee must also prepare the FD-1053 in the database for reporting purposes but does not need to generate the request letter.

18.6.8.5.2 (U) DURATION OF APPROVAL

(U) As authorized by statute (e.g., for as long as the emergency necessitating usage exists and only in those circumstances when it is impracticable to obtain other legal process such as a subpoena or NSL) and applicable court order or warrant.

18.6.8.5.3 (U) SPECIFIC PROCEDURES

- A) (U//FOUO) **Required Form:** An FD-1053 Form must be used by all employees to document requests for emergency voluntary disclosures of information. The FD-1053 Form will automatically generate a letter which the FBI can furnish to the particular electronic communications service provider. The FD-1053 Form must also be used to document those instances when a provider independently discloses emergency information without an initial request from the FBI. In such a situation, the FD-1053 system will not generate, and the FBI need not send, an emergency voluntary disclosure letter to the provider.

- B) (U//FOUO) **Filing requirements:** A copy of each document used to obtain disclosure of information pursuant to the authorities under ECPA, e.g., the FD-1053 Form, the emergency disclosure letter or the electronic communications service provider's standardized form, must be serialized in the investigative file, along with documentation of any information obtained in response to the request.
- C) (U//FOUO) **Contact with Providers:** TTAs have primary responsibility for liaison with a provider's legal compliance staff and are, therefore, typically familiar with procedural requirements of the various providers. FBI employees should contact the TTA and the CDC or OGC for guidance and with questions relative to process and procedures for serving compulsory process or requesting voluntary disclosures.

18.6.8.5.4 (U) COST REIMBURSEMENT

(U) Policy and procedures regarding cost reimbursement are described in the following:

- A) (U) Standardized payment procedures may be found at <http://home.fbinet.fbi/DO/OGC/Main%20Law%20Library/Forms/ILU%20Library.aspx>
- B) (U) Cost Reimbursement Guidance can also be found in 18 U.S.C. § 2706 http://home.fbinet.fbi/DO/OGC/Main%20Law%20Library/cost_reimbursement_guidance.pdf

18.6.8.5.5 (U) NOTICE AND REPORTING REQUIREMENTS

18.6.8.5.6 (U) REPORTING VOLUNTARY EMERGENCY DISCLOSURES

(U) 18 U.S.C. § 2702(d) requires the Attorney General to report annually to Congress information pertaining to the receipt of voluntary disclosures of the contents of stored wire or electronic communications in an emergency under 18 U.S.C. § 2702(b)(8), specifically:

- A) (U) The number of accounts from which the FBI received voluntary emergency disclosures; and
- B) (U) A summary of the basis for the emergency disclosure in those investigations that were closed without the filing of criminal charges.

(U) The FD-1053 Form will capture information required to meet these reporting requirement.

18.6.8.5.7 (U) ROLES/RESPONSIBILITIES

(U) The FD-1053 database system that hosts the FD-1053 form will, when necessary, follow-up with e-mail notifications to the issuing employee to ensure that the information included in the report to DOJ (which it uses to prepare the required Congressional report) is current. It is the responsibility of the FBI employee to respond to these requests for information as soon as practicable but no later than ten (10) business days. Failure to do so may be considered "substantial non-compliance" pursuant to Section 3.

(U) OGC/ILB is assigned the administrative responsibility to complete the following by December 31 of each year:

- A) (U) Tabulate the number of voluntary disclosures of stored contents received under the authority of 18 U.S.C. § 2702(b)(8) for the calendar year;

§18

Domestic Investigations and Operations Guide

- B) (U) Prepare a report summarizing the basis for disclosure in those instances in which the relevant investigation was closed without the filing of criminal charges; and
- C) (U) Submit the report to the General Counsel for review and submission to DOJ according to the statutory requirement for annual report by the Attorney General.

18.6.8.6 (U) OTHER APPLICABLE POLICIES

(U) See the Stored Communications Quick Reference Guide 5-1-2008

18.6.9 (U) INVESTIGATIVE METHOD: PEN REGISTERS AND TRAP/TRACE DEVICES (PR/TT)

18.6.9.1 (U) SUMMARY

(U) Pen register and trap and trace (PR/TT) devices enable the prospective collection of non-content traffic information associated with wire and electronic communications, such as: the phone numbers dialed from or to a particular telephone, including electronic communications; messages sent from or to a particular telephone; or the internet protocol (IP) address of communications on the Internet and other computer networks.

18.6.9.2 (U) APPLICATION

(U//FOUO) The PR/TT may be used in Preliminary and Full (national security and criminal) Investigations. This method may not be used: (i) for targeting an USPER when providing assistance to other agencies, unless there is already an open FBI Preliminary or Full Investigation related to the request for assistance or the predicate exists to open a Preliminary or Full Investigation; (ii) for targeting an USPER when collecting against a foreign intelligence requirement; or (iii) during an Assessment.

18.6.9.3 (U) LEGAL AUTHORITY

(U) 18 U.S.C. §§ 3121 et seq. and 50 U.S.C. §§ 1842 et seq. regulate the use of PR/TT devices. PR/TT orders authorize the collection of phone number dialed from or to a particular telephone, IP addresses, port numbers and the “To” and “From” information from e-mail; they cannot intercept the content of a communication, such as telephone conversations or the words in the “subject line” or the body of an e-mail.

18.6.9.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) A pen register device or process records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication. See 18 U.S.C. § 3127(3).

(U) A trap and trace device or process captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication. See 18 U.S.C. § 3127(4).

18.6.9.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

18.6.9.5.1 (U) PEN REGISTER/TRAP AND TRACE UNDER FISA

(U) Applications for authority to use a PR/TT device can be made to the FISC in national security investigations. See 50 U.S.C. § 1842.

18.6.9.5.1.1 (U) LEGAL STANDARD

(U) Applications to the FISC are to be under oath and must include:

A) (U) The identity of the federal officer making the application; and

B) (U) A certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning an USPER or is information that is relevant to an ongoing investigation to protect the United States against international terrorism or clandestine intelligence activities; and that such investigation, if of an USPER, is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

18.6.9.5.1.2 (U) PROCEDURES

(U//FOUO) Requests for opening or renewal of FISA PR/TT must be made using FISAMS and a standard "FISA Pen Register/Trap and Trace Request Form" for review by an attorney of the NSLB, OGC. For field offices/divisions with SCION access, Top Secret and/or SCI (including Secret SCI) level requests must be submitted through FISAMS on SCION. Field offices/divisions without SCION access must submit their Top Secret and/or SCI requests through appropriate secure channels (e.g., courier or secure fax). FISAMS will route the request to appropriate parties for their review and approval of the request as it proceeds from the field through FBIHQ, DOJ, and FISC. Routing a paper copy for signatures is not required.

18.6.9.5.1.3 (U) EMERGENCY AUTHORITY—FISA: 50 U.S.C. § 1843

(U//FOUO) Under the provisions of FISA, the Attorney General may grant Emergency Authority (EA) for PR/TT. Requests for Emergency Authority must be referred to the appropriate FBIHQ division.

(U//FOUO) Because of the expedited nature of these requests, they are generally handled by telephone or in person and not through FISAMS. In order to track the resulting court docket and create a record for renewal purposes, FISAMS has an express process that allows the FISA unit to create a tracking record and upload the resulting court orders or warrants. The express process can only be entered by the FISA unit at FBIHQ. After an emergency package and supporting FISA order are obtained, contact the FISA unit to ensure the package is entered into FISAMS.

A) (U) The Attorney General may authorize the installation and use of a PR/TT upon a determination that an emergency exists and that the factual basis exists for a court order. The FISC must be informed at the time of the authorization and an application for a court order must be made to the court as soon as practicable, but no more than seven (7) days after the authorization. If the court does not issue an order approving the use of a PR/TT, an emergency-authorized PR/TT use must terminate at the earliest of when the information sought is obtained, when the FISC denies the application, or seven (7) days after the Attorney General authorization is given.

B) (U) If the FISC denies the application after an emergency PR/TT device has been installed, no information collected as a result may be used in any manner, except with the approval of the Attorney General upon a showing that the information indicates a threat of death or serious bodily harm to any person..

(U) Notwithstanding the foregoing, the President, acting through the Attorney General, may authorize the use of a PR/TT, without a court order, for a period not to exceed 15 calendar days, following a declaration of war by Congress. See 50 U.S.C. § 1844.

(U//FOUO) For an emergency authorization to use a PR/TT surveillance, DOJ OI can be reached during regular business hours at (202) 514-5600 or through the DOJ Command Center at (202) 514-5000 at any time.

18.6.9.5.1.4 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization (“FISA overcollection”) will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.6.9.5.2 (U) CRIMINAL PEN REGISTER/TRAP AND TRACE UNDER TITLE 18

(U) Applications for the installation and use of a PR/TT device may be made to a “court of competent jurisdiction”—i.e., “any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated, or any court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or trap and trace device.” See 18 U.S.C. § 3127(2).

18.6.9.5.2.1 (U) LEGAL STANDARD

(U) Applications for authorization to install and use a PR/TT device must include:

- A) (U) The identity of the attorney for the government or the state law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- B) (U) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18.6.9.5.2.2 (U//FOUO) PROCEDURES

(U//FOUO) An SSA must approve a request for opening or renewal of PR/TT use by EC prior to submission of the request to an attorney for the government. Before approving such a request, the SSA should consider of the following:

- A) (U//FOUO) The use of resources based on the investigative purpose set forth;
- B) (U//FOUO) Whether there is sufficient factual basis for the certification to be made in the application (i.e., is the information likely to be obtained relevant to an ongoing criminal investigation);
- C) (U//FOUO) Whether the customer or subscriber has consented to the use of a PR/TT, see 18 U.S.C. § 3121(b)(3); or

D) (U//FOUO) Whether the use of a PR/TT is the least intrusive method if reasonable and effective based upon the circumstances of the investigation.

(U//FOUO) A copy of the approving EC must be maintained in the pen register sub-file "PEN."

(U//FOUO) A PR/TT order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the government or law enforcement or investigative officer that is serving the order must provide written or electronic certification that the order applies to the person or entity being served.

18.6.9.5.2.3 (U) EMERGENCY AUTHORITY—CRIMINAL: 18 U.S.C. § 3125

(U) The Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General may specially designate any investigative or law enforcement officer to reasonably determine whether an emergency situation exists that requires the installation and use of a PR/TT device before an order authorizing such installation and use can, with due diligence, be obtained and there are grounds upon which an order could be entered authorizing the installation and use of a PR/TT.

(U) An emergency situation as defined in this section involves:

A) (U) Immediate danger of death or serious bodily injury to any person;

B) (U) Conspiratorial activities characteristic of organized crime;

C) (U) An immediate threat to a national security interest; or

D) (U) An ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year.

(U) Only DOJ officials have the authority to authorize the emergency installation of a PR/TT. The FBI does not have this authority. If the DOJ authorizes the emergency installation of a PR/TT, the government has 48 hours after the installation to apply for and obtain a court order according to 18 U.S.C. § 3123. It is a violation of law to fail to apply for and obtain a court order within this 48 hour period. Use of the PR/TT shall immediately terminate when the information sought is obtained, when the application for a court order is denied, or if no court order has been obtained 48 hours after the installation of the PR/TT device in emergency situations.

(U//FOUO) As with requesting authorization for an emergency Title III, DOJ prefers for the AUSA to contact the DOJ Criminal Division Office of Enforcement Operations (OEO) to request an emergency PR/TT. After discussions with the AUSA, the DOJ attorney in consultation with the OEO Director or an Associate Director will determine whether the statutory requirements have been met. If so, the DOJ attorney will contact the appropriate Criminal Division official and obtain authorization to proceed. Once that

approval has been obtained, the DOJ attorney will advise the AUSA that the emergency use has been approved and that the law enforcement agency may proceed with the installation and use of the PR/TT. The DOJ attorney will send a verification memorandum, signed by the authorizing official, to the AUSA. The AUSA will include an authorization memorandum with the application for the court order approving the emergency use.

(U//FOUO) If an emergency situation arises after regular business hours, an attorney at DOJ OEO, Electronic Surveillance Unit (ESU) may be reached through the Department of Justice Command Center at (202) 514-5000. During regular business hours, the ESU may be reached at (202) 514-6809; facsimile (202) 616-8256.

18.6.9.6 (U) DURATION OF APPROVAL

- A) (U) **FISA:** The use of a PR/TT device may be authorized by the FISC for a period of time not to exceed 90 days in investigations targeting an USPER. Extensions may be granted for periods not to exceed 90 days upon re-application to the court. In investigations in which the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person (USPER), an order or extension may be for a period of time not to exceed one year.
- B) (U) **Criminal:** The installation and use of a PR/TT device may be authorized by court order under 18 U.S.C. § 3123 for a period not to exceed 60 days, which may be extended for additional 60-day periods.

18.6.9.7 (U) SPECIFIC PROCEDURES

(U//FOUO) Prior to installing and using a PR/TT device (whether issued in a criminal or national security matter), the case agent must:

- A) (U//FOUO) Coordinate with the technical advisor in advance of seeking approval or court order authority for the use of a PR/TT device to discuss required capabilities and submit an electronic technical request form to the technical advisor or the technical supervisor for use of the equipment or technique. Before executing the technical request, the technical advisor or technical supervisor must ensure that the PR/TT may be affected according to the authorizing order or other statutory authority. The TTA is: (i) the primary point of contact for liaison with the carrier or provider; (ii) responsible for coordinating the intercept; and (iii) will order any necessary assistance from the provider.
- B) (U//FOUO) File a copy of each application and the order authorizing use of the PR/TT in the pen register sub-file "PEN."
- C) (U//FOUO) Ensure that the court order and cost information is entered into the Technical Management Database (TMD) so it can be tracked and managed according to policy requirements.
- D) (U//FOUO) For criminal PR/TT devices, ensure that upon termination of the coverage, the information required to be reported to Congress under 18 U.S.C. § 3126 is reported to FBIHQ using the Court Order Module in TMD. For all criminal PR/TT orders or extensions issued on or after January 1, 2009, the TMD must be used to capture the required report information. PR/TT devices used pursuant to consent or under the provisions of FISA are not included in the report to Congress.

- E) (U//FOUO) Ensure that the data collected is promptly loaded electronically into Telephone Applications and any other applicable system.

18.6.9.8 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that use authority be obtained for foreign proceedings as well. Questions concerning the FISA use policy or requests for assistance in obtaining FISA use authority from the AG should be directed to NSLB’s Classified Litigation Support Unit.

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the “aggrieved person” [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.6.9.9 (U) CONGRESSIONAL NOTICE AND REPORTING REQUIREMENTS

18.6.9.9.1 (U) CRIMINAL PEN REGISTER/TRAP AND TRACE- ANNUAL REPORT

(U) The Attorney General is required to make an annual report to Congress on the number of criminal PR/TT orders applied for by DOJ law enforcement agencies. See 18 U.S.C. § 3126. The report must include the following information:

- A) (U) The period of interceptions authorized by the order, and the number and duration of any extensions;
- B) (U) The offense specified in the order or application, or extension;
- C) (U) The number of investigations involved;
- D) (U) The number and nature of the facilities affected; and
- E) (U) The identity, including the district, of the applying agency making the application and the person authorizing the order.

(U//FOUO) DOJ, Criminal Division, OEO requires the FBI to provide quarterly reports on pen register usage. To satisfy DOJ data requirements and standardize and simplify field reporting, court-ordered pen register usage must be reported to FBIHQ using the Court Order Module in TMD, “Pen Register/Trap and Trace Usage” within five (5) workdays after the expiration date of an original order and any extensions, or denial of an application for an order. For all criminal PR/TT orders or extensions issued on or after January 1, 2009, the

TMD must be used to capture the required report information. These reporting requirements do not apply to PR/TT authorized pursuant to consent or under the provisions of FISA.

18.6.9.9.2 (U) NATIONAL SECURITY PEN REGISTERS AND TRAP AND TRACE – SEMI-ANNUAL

(U) The Attorney General must inform the House Permanent Select Committee on Intelligence, Senate Select Committee on Intelligence, Committee of the Judiciary of the House Representatives, and Committee of the Judiciary of the Senate concerning all uses of PR/TT devices pursuant to 50 U.S.C. § 1846. This report is coordinated through DOJ NSD. A semi-annual report must be submitted that contains the following information:

- A) (U) The total number of applications made for orders approving the use of PR/TT devices;
- B) (U) The total number of such orders either granted, modified, or denied; and
- C) (U) The total number of PR/TT devices whose installation and use was authorized by the Attorney General on an emergency basis and the total number of subsequent orders approving or denying the installation and use of such PR/TT devices.

18.6.9.10 (U) POST CUT-THROUGH DIALED DIGITS (PCTDD)

18.6.9.10.1 (U) OVERVIEW

(U//FOUO) Telecommunication networks provide users the ability to engage in extended dialing and/or signaling (also known as "post cut-through dialed digits" or PCTDD), which in some circumstances are simply call-routing information and, in others, are call content. For example, non-content PCTDD may be generated when a party places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. In other instances, PCTDD may represent call content, such as when a party calls an automated banking service and enters an account number, calls a pharmacy's automated prescription refill service and enters prescription information, or enters a call-back number when prompted by a voice mail service. See United States Telecom Assn v. Federal Communications Commission, 227 F.3d 450, 462 (D.C. Cir. 2000). After the initial "cut-through," a pen register and the equipment that supports it cannot tell the difference between digits that are dialed to connect a call and those that would otherwise be considered content.

(U//FOUO) The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." See 18 U.S.C. § 3127(3) and (4). In addition, 18 U.S.C. § 3121(c) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purport, or meaning of a communication. See 18 U.S.C. § 2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the extent feasible, any possible over collection of content while still allowing the device to collect all of the dialing and signaling information authorized.

(U//FOUO) **DOJ Policy:** In addition to this statutory obligation, DOJ has issued a directive in the form of a DAG Memo (see below paragraph) to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

(U//FOUO) Although the DAG Memo, dated May 24, 2002 on “Avoiding Collection and Investigative Use of “Content” in the Operation of Pen Registers and Trap and Trace Devices,” as written, applies only to the issuance of criminal pen register orders pursuant to 18 U.S.C. § 3121 et seq., the potential collection of PCTDD-content also exists for pen registers authorized under FISA. As such, the principles outlined in the DAG Memo apply to pen registers authorized pursuant to the FISA as well as pen registers authorized pursuant to Title 18 of the United States Code. **In instances in which PCTDD are collected pursuant to FISA, the government may not make any affirmative investigative use of the information, even in cases of emergency, without authorization from the FISC.** Any such emergency use must be recorded in the respective investigative files.

18.6.9.10.2 (U) COLLECTION OF PCTDD

(U//FOUO) When requesting pen register collection, the field office case agent must affirmatively decide whether to receive PCTDD during the course of a pen register collection. If no selection is made, the default is set not to collect PCTDD.

- A) (U//FOUO) The case agent shall, consistent with DIOG Section 18.6.9.10.1, submit an electronic technical request form that states whether PCTDDs are to be collected—for example, when the order authorizes the “recording or decoding of all dialing, routing, addressing, or signaling information.” This selection is accomplished by marking the “Post Cut through Dialed Digits Authorized” check box for each monitored target. If this selection is not made, the PCTDD will not be collected or presented in any collection report.
- B) (U//FOUO) The case agent shall advise the technically trained agent (TTA) promptly upon learning that a particular pen register order expressly prohibits the collection or retention of PCTDD. The technical agent shall then take all reasonable steps to ensure compliance with the restrictive order, including coordinating with the service provider and with OTD personnel regarding the use of technology reasonably available to avoid the collection of all PCTDD.

18.6.9.10.3 (U) USE OF PCTDD

(U//FOUO) If PCTDD information is collected pursuant to an authorized pen register, the following steps must be taken by all FBI personnel when reviewing pen register derived information to avoid the use of the contents of communications that may be contained within the string of digits:

- A) (U//FOUO) Prior to examining any PCTDD, identify—through use of administrative subpoena or other investigative means—the subscriber of the phone number to whom the initial connection was made (i.e., the origination number).
 - 1) (U//FOUO) If the origination number does not appear to be pertinent to the investigation, no examination of any PCTDD associated with that initial phone number shall be made, absent an investigative need to examine the PCTDD.

- 2) (U//FOUO) If the initial connection is determined to be to a financial institution as defined in the Right to Financial Privacy Act, 12 U.S.C. § 3401(1), PCTDD may not be examined, because there is reason to believe that the PCTDD may contain the contents of a communication, such as a bank account number.
 - 3) (U//FOUO) The fact that the target called the bank, however, can be used for investigative or intelligence purposes, such as to subpoena bank records associated with the target; but any PCTDD cannot be used in the subpoena (such as a bank account number) or later to confirm information received from the bank.
 - 4) (U//FOUO) If the initial connection is determined to be an entity for which it is reasonable to believe that the PCTDD would contain dialing or signaling information, such as a calling card number, a call spoof card service, a company otherwise providing direct access to a telephone service, or a business entity, the PCTDD may be examined to identify the ultimate destination of the call, or any other associated signaling or routing information, such as a calling card PIN or calling card account number. If the initial connection is to a business entity, like a hotel, for example, the PCTDD may be examined to determine if an extension number was dialed.
 - 5) (U//FOUO) If, when examining PCTDD, numbers are encountered that constitute “content” of a communication, except as provided below, those numbers may not be used for any affirmative investigative purpose. In essence, those numbers must be treated as though they did not exist and cannot be used for any purpose. To the extent the information is included in any document for analytic or investigative use, the PCTDD numbers that constitute “content” must be redacted.
- B) (U//FOUO) **Emergency Use:** In an emergency, PCTDD that constitutes content may be used as necessary in criminal investigations to prevent immediate danger of death, serious physical injury, or harm to the national security. **In instances in which PCTDD are collected pursuant to FISA, the government may not make any affirmative investigative use of the information, even in cases of emergency, without authorization from the FISC.**
- 1) (U//FOUO) **Approval:** In criminal investigations only, an SSA or SIA, who reasonably determines that an emergency situation exists that requires the use of PCTDD content relating to the emergency, may approve the use of such PCTDD without delay.
 - 2) (U//FOUO) **Notification:** Within five (5) business days of such emergency use, the use of the particular PCTDD content must be documented in an EC to the appropriate investigative files (i.e., the investigation in which the pen register information was derived and the investigation in which it was used) with notification to the CDC and the FBI General Counsel, OGC (Investigative Law Unit for criminal pen registers and National Security Law Branch for FISA pen registers).

18.6.9.10.4 (U) WHAT CONSTITUTES PCTDD CONTENT

(U//FOUO) In applying the above, the term “content” is interpreted to mean “any information concerning the substance, purport, or meaning of a communication” as defined in 18 U.S.C. § 2510. Questions concerning whether specific PCTDD are content as opposed to dialing, routing, addressing, or signaling information should be addressed to the CDC or OGC for coordination with DOJ as necessary.

(U//FOUO) **Exemption:** This policy does not pertain to e-mail or Internet account pen register surveillance because such electronic communications do not generate PCTDD. Nor does the policy pertain to PCTDD obtained pursuant to a Title III or FISA electronic surveillance

order, because such orders authorize the interception of contents of communications associated with the targeted phone number.

18.6.9.11 (U//FOUO) CELL SITE SIMULATORS/DIGITAL ANALYZERS/WIRELESS INTERCEPT TRACKING TECHNOLOGY

(U//FOUO) A PR/TT order is required (absent consent of the wireless phone user) for the FBI to use equipment to capture any "signaling information"—including the Mobile Station Identification Number (MSIN) and Electronic Serial Number (ESN) or other registration-type data—emitted from a wireless phone into the public airspace—even though this can be accomplished without the assistance of the service provider. Because 18 U.S.C. § 3127 defines PR/TT devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, the government's use of its own device to capture such signaling data—whether passively monitoring or actively interrogating—constitutes the use of a "pen register" device and requires an order or statutory exception to avoid violating the statute. The following discusses how wireless intercept tracking technology (WITT) is used:

18.6.9.11.1 (U//FOUO) To LOCATE A KNOWN PHONE NUMBER

- A) (U//FOUO) **Authority:** A standard PR/TT order issued pursuant to 18 U.S.C. § 3127 is adequate to authorize the use of this technology to determine the location of a known targeted phone, provided that the language authorizes FBI employees to install or cause to be installed and use a pen register device, without geographical limitation, at any time of day or night within (X) days from the date the order is signed, to record or decode dialing, routing, addressing, or signaling information transmitted by the "Subject Telephone." Due to varying and often changing court interpretations of the requirements for obtaining cell site location information, agents contemplating legal process to obtain such information should consult as necessary with their CDC and/or AUSA for the legal requirements in their particular jurisdiction. The application and order should generally also request authority to compel disclosure of cell site location data on an ongoing basis under 18 U.S.C. § 2703(d)—or probable cause, if such is required by the particular district court—as such information may assist in determining the general location of the targeted phone. FISA PR/TT orders do not currently authorize the collection of cell site location information.
- B) (U//FOUO) **Surveillance aid:** Traditionally, this equipment has been deployed only as a surveillance aid. Using the results as evidence is generally discouraged because of the level of technical expertise required to effectively operate the equipment. Accordingly, FBI employees should corroborate and verify the information obtained through other means (e.g., pretext calls, CHS information, and MST surveillance) that can be used as evidence in any court filing (e.g., Title III affidavit, search warrant affidavit). FBI employees may not make affirmative investigative use of signaling information inadvertently acquired that is known to have emanated from a private residence, unless it is necessary to prevent an immediate danger of death, serious physical injury, or harm to the national security.
- C) (U//FOUO) **Targeting a residence:** The deliberate use of this technology to determine whether a targeted phone is operating within a particular residence could be deemed to constitute a search under the Fourth Amendment. There is, however, currently no specific decision on point. The sale and use of this type of equipment is controlled as "surreptitious interception" equipment under 18 U.S.C. § 2512. Accordingly, its authorized use is typically restricted to law enforcement or government and service providers for use in the normal course of business. It is likely, therefore, that such equipment would not be considered "in

general public use.” Under Kyllo v. United States, 533 U.S. 27 (2001), the use of equipment not in general public use to acquire data that is not otherwise detectable that emanates from a private premise implicates the Fourth Amendment. If so, the use of such equipment to target a particular residence to determine whether a particular cellular phone is operating inside the residence would constitute a search for purposes of the Fourth Amendment.

- D) 1. (U//FOUO) In the absence of clear law, such equipment should not be intentionally used to target a private premise to determine whether a particular targeted phone is operating inside nor be used to determine whether a targeted cellular phone is operating from within a particular private premise, absent consent, exigent circumstances or a search warrant for the phone (a search warrant in this circumstance would be similar to an anticipatory search warrant for a tracking device). Prior consultation with the AUSA involved in the investigation concerning the particular factual circumstances, however, may result in a determination that a warrant is not necessary. In the event a search warrant is obtained, consideration should be given to requesting delayed notice (18 U.S.C. § 3103a), to relying on corroborating techniques to confirm the existence of the phone, and to claiming a privilege against disclosure of the investigative technique based on the likely adverse result such disclosure would have on the future viability of the technique for investigations.

18.6.9.11.2 (U//FOUO) To IDENTIFY AN UNKNOWN TARGET PHONE NUMBER

(U//FOUO) **Authority:** A pen register order is required when this technology is used to identify an unknown target phone number. The pen register application should explain that the device is used to detect registration signaling data from multiple phones, to include non-target phones, at locations in which the target telephone is reasonably believed to be operating and then the recurrence of a common number is correlated to the presence of the target. Once the target number is identified, all non-target numbers are to be purged in order to protect the privacy of those non-targets, as well as to preserve promptly the operational use of the equipment. Hence, although the non-target data may be temporarily acquired, it is not maintained beyond that necessary to effect the pen register, e.g., to identify the targeted phone. No affirmative use of such incidentally acquired non-target data is permitted.

(U//FOUO) If active interrogation is to be used to identify a target phone, the pen register application should also advise the court of the potential for temporary disruption of service and state that, e.g., “any potential interference to service occasioned by use of the Pen Register or Trap and Trace will be minimized so as to be no more disruptive than might ordinarily occur with cellular service coverage.” (Note that there is no interference when the device is used to passively monitor RF signals.) A temporary disruption can be caused because when a phone registers with the device, it cannot simultaneously register with the provider’s network. Consequently, the phone may experience a temporary disruption in service during the brief time that it is “registered” with the device—not unlike a typical lapse in cellular service occasionally experienced by the average cell phone user (e.g., dropped calls). Such a brief delay in coverage may be considered so de minimis as to be legally insignificant. Nonetheless, informing the court in the application of the potential for interference serves two objectives:

- A) (U//FOUO) Addresses the pen register statutory requirement that a pen register device be installed and used “with a minimum of interference with the services” accorded to the target of the pen register (18 U.S.C. § 3124(a)); and

- B) (U//FOUO) Addresses potential claim based on Section 333 of title 47 of the United States Code, which provides "No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed" by the FCC—to include commercial cellular frequencies. This prohibition is arguably inapplicable to the use of this device by the government because the government is not included within the definition of "person." See 47 U.S.C. § 153(32).

18.6.9.11.3 (U) PR/TT ORDER LANGUAGE

- (U) The language in the order should state that "the pen register will be implemented unobtrusively and with minimum interference with the services accorded to customers of such service."

18.6.10 (U) INVESTIGATIVE METHOD: MAIL COVERS

18.6.10.1 (U) SUMMARY

(U) A mail cover may be sought only in a Predicated Investigation when there are reasonable grounds to demonstrate that the mail cover is necessary to: (i) protect the national security; (ii) locate a fugitive; (iii) obtain evidence of the commission or attempted commission of a federal crime; or (iv) assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law. See 39 C.F.R. § 233.3(e)(2).

(U) Subject to the requirements in this section, a criminal or national security mail cover may be sought on any person or entity, including but not limited to the subject of the investigation, when there are reasonable grounds to believe it is necessary to achieve one or more of the above-listed goals and the results of the mail cover are reasonably anticipated to be "relevant to" the Predicated Investigation.

(U) A mail cover may be sought only from the United States Postal Service (USPS); a mail cover may not be requested from package carriers (e.g., Federal Express, United Parcel Service) that do not handle mail processed through the USPS. Nor may mail covers be requested from the military postal system overseas or from persons performing military postal duties overseas. As a general rule, a mail cover in the APO/FPO system overseas may only be ordered by a military authority competent to order searches and seizures for law enforcement purposes, usually a commanding officer. See DOD 4525.6-M, the DOD Postal Manual.

18.6.10.2 (U) APPLICATION

(U//FOUO) Mail covers may be used in Predicated Investigations, to include those opened to provide assistance to other agencies (consult the CDC or FBIHQ OGC for further guidance for assistance to other agencies). A mail cover cannot be used to collect positive foreign intelligence. A mail cover cannot be used during an Assessment.

18.6.10.3 (U) LEGAL AUTHORITY

- A) (U) Postal Service Regulation 39 C.F.R. § 233.3 is the sole authority and procedure for opening a mail cover and for processing, using and disclosing information obtained from a mail cover;
- B) (U) There is no Fourth Amendment protection for information on the outside of a piece of mail. See, e.g., U.S. v. Choate, 576 F.2d 165, 174 (9th Cir., 1978); and U.S. v. Huie, 593 F.2d 14 (5th Cir., 1979); and
- C) (U) AGG-Dom, Part V.A.2.

18.6.10.4 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) A mail cover is the non-consensual recording of any data appearing on the outside cover of any sealed or unsealed mail matter to obtain information in order to:

- A) (U) Protect the national security;
- B) (U) Locate a fugitive;

- C) (U) Obtain evidence of commission or attempted commission of a federal crime;
- D) (U) Obtain evidence of a violation or attempted violation of a postal statute; or
- E) (U) Assist in the identification of property, proceeds or assets forfeitable under law.
See 39 C.F.R. § 233.3(c)(1).

(U) In this context, a “recording” means the transcription, photograph, photocopy, or other facsimile of the image of the outside cover, envelope, or wrappers of mailed matter. A warrant or court order is almost always required to obtain the contents of any class of mail, sealed or unsealed.

18.6.10.5 (U) STANDARD FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U) The standard to obtain a mail cover is established by the Postal Service regulation. The Chief Postal Inspector may order a mail cover “[w]hen a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to:

- A) (U) Protect the national security;
- B) (U) Locate a fugitive;
- C) (U) Obtain information regarding the commission or attempted commission of a crime; or
- D) (U) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.” See 29 C.F.R. § 233.3(e)(2).

(U//FOUO) **National Security Mail Cover:** A national security mail cover request may be approved by the field office ADIC or SAC or at Headquarters by the EAD of the National Security Branch. A national security mail cover sought “to protect the national security” includes protecting the United States from actual or threatened attack or other grave, hostile act; sabotage; international terrorism; or clandestine intelligence activities, including commercial [economic] espionage by foreign powers or their agents.

(U//FOUO) After SSA approval, a national security mail cover request must be reviewed for legal sufficiency by an FBI attorney (i.e., CDC, ADC, or OGC NSLB attorney) before it may be approved by an ADIC or SAC (including anyone who is officially in an acting ADIC or SAC capacity) or the EAD of the National Security Branch (approval cannot be delegated).

(U//FOUO) **Required Form:** The **FD-1064a** must be used for all National Security Mail Covers.

(U//FOUO) **Criminal Mail Cover:** A criminal mail cover request may be approved by the field office SSA. The SSA may approve a request for a mail cover if there are reasonable grounds to demonstrate that the mail cover is necessary to assist in efforts to: (i) locate a fugitive; (ii) obtain information regarding the commission or attempted commission of a federal crime; or (iii) to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

(U//FOUO) **Required Form:** The **FD-1064** must be used for all Criminal Mail Covers.

(U//FOUO) Review and Approval of National Security or Criminal Mail Cover Requests:

Approval of any mail cover request or extension is conditioned on the following criteria being met:

- A) (U//FOUO) The request states a reasonable ground to demonstrate the mail cover is necessary to: (i) locate a fugitive; (ii) obtain information regarding the commission or attempted commission of a federal crime; (iii) assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law; or (iv) protect the national security.
- B) (U//FOUO) The request for the mail cover includes the full name and complete address, to include postal ZIP Code, if known, of the mail to be covered. If the name of the mail recipient is unknown, the request includes an explanation of why obtaining information regarding mail addressed to the targeted address is necessary to accomplish the authorized objective of the mail cover. If other individuals using the same address are not to be covered, the request includes those names and the fact that they should be excluded from coverage.
- C) (U//FOUO) In a national security investigation, if a mail cover is requested on an organization, the request states, if known, whether the organization is organized under the laws of the United States or foreign laws and whether any United States persons (USPERs) or non-United States persons (non-USPERs) work there. The request specifically names USPERs not to be covered, if appropriate. If the subject is a foreign establishment or corporation, the request lists and excludes, if necessary, the USPERs working in the establishment, to the extent the information is known.
- D) (U//FOUO) If the request is to obtain information regarding the commission or attempted commission of a federal crime, the request: (i) cites the specific criminal statute, with a description of the violation, the penalty for the violation, and the nexus between the investigation and each address/subject; (ii) sets forth how the subject of the mail cover is violating the statute or how the subject is otherwise connected to the investigation; and (iii) explains how the mail cover will facilitate the investigation, e.g., identify the location of property or assets for forfeiture by revealing banking information.
- E) (U//FOUO) The request describes the classes of mail to be covered, including whether outgoing and/or incoming mail is to be covered. Classes of mail to be covered beyond first class must be specifically requested and justified according to the "reasonable grounds" standard articulated in the Postal Service regulation. See 39 C.F.R. § 233.3(e)(2).
- F) (U//FOUO) If the subject of the mail cover is represented by legal counsel or under indictment, the request provides the name and address of legal counsel, if known. Under postal regulations, a mail cover must not include matter mailed between the mail cover subject and the subject's attorney, unless the attorney is also a subject under the investigation.
- G) (U//FOUO) The request states the duration for which the mail cover is requested and notes that the authorized period begins on the date the request is instituted by the local post office.
- H) (U//FOUO) The request specifies the name and address of the individual to whom the results of the mail cover should be forwarded.
- I) (U//FOUO) The request specifies mechanical reproduction (photocopying) only when necessary and, if photocopying is requested, must include a statement to the effect that: "The nature of the language or writing on envelopes often makes it difficult to transcribe;" or, in

exceptional cases, a statement to the effect that: "Because the return address and other physical features of some envelopes addressed to the subject are known to contain secret writing and/or clandestine instructions, it is requested that this mail cover include mechanical reproduction of both sides of all first class and priority envelopes addressed to the subject."

(U) **Emergency Requests:** When time is of the essence, the Chief Postal Inspector, or designee, may act upon an oral request to be confirmed by the requesting authority, in writing, within three calendar days. Information may be released prior to receipt of the written request only when the releasing official is satisfied that an emergency situation exists. See 39 C.F.R. § 233.3(e)(3).

(U) An "emergency situation" exists when the immediate release of information is required to prevent the loss of evidence or when there is a potential for immediate physical harm to persons or property. See 39 C.F.R. § 233.3(c)(10).

18.6.10.6 (U) DURATION OF APPROVAL

- A) (U) **National Security Mail Covers:** No national security mail cover may remain in force for longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or his/her designees at National Headquarters. See 39 C.F.R. § 233.3(g)(6).
- B) (U) **Criminal Mail Covers Except Fugitives:** A mail cover in a criminal investigation is limited to no more than 30 days, unless adequate justification is provided by the requesting authority. See 39 C.F.R. § 233.3(g)(5). Renewals may be granted for additional 30-day periods under the same conditions and procedures applicable to the original request. The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from the extension.
- C) (U) **Fugitives:** No mail cover instituted to locate a fugitive may remain in force for longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or his/her designees at National Headquarters. See 39 C.F.R. § 233.3(g)(6).
- D) (U) **Exception for Indictments and Information:** Except for fugitive investigations, no mail cover may remain in force when an information has been filed or the subject has been indicted for the matter for which the mail cover has been requested. If the subject is under investigation for further criminal violations, or a mail cover is required to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested. See 39 C.F.R. § 233.3(g)(7). Any mail cover results pertaining to the subject(s) provided by the USPS after an indictment or information is filed cannot be used for investigative purposes or uploaded by the FBI (other than the exception regarding fugitives), and shall be returned promptly to the USPS.

18.6.10.7 (U) STORAGE OF MAIL COVER INFORMATION

(U//FOUO) The Postal Regulation requires that physical storage of all reports issued pursuant to a mail cover request to be at the discretion of the Chief Postal Inspector. See 39 C.F.R. § 233.3(h)(1). Accordingly, FBI employees must conduct a timely review of mail cover documents received from the USPS. A copy of the signed mail cover request and the signed transmittal letter must be maintained in the investigative file.

18.6.10.8 (U) RETURN OF MAIL COVER INFORMATION TO USPS

(U//FOUO) Current USPS policy guidance for a mail cover in a criminal investigation requires return to the USPS of all documentation provided by the USPS in a mail cover and prohibits copying and retention of these documents. The documents should be returned to the *USPS after final adjudication and/or the closing of the investigation; the fact that materials* were returned to USPS must be documented in the investigative file. This policy guidance does not apply to a national security mail cover.

18.6.10.9 (U) COMPLIANCE AND MONITORING

(U//FOUO) FBI employees must conduct a timely review of mail cover information received from the USPS for any potential production of data beyond the scope of the requested mail cover ("overproduction"). Overproduced information from a mail cover must not be uploaded into any FBI database or used in any manner.

- A) (U//FOUO) **Criminal Mail Cover – Overproduction:** Overproduced information must be returned with a letter to the assigned to the USPS entity from which it was obtained stating the reason(s) for the return. Destruction of the overproduced material is not an option under the current Postal regulations.
- B) (U//FOUO) **National Security Mail Cover – Overproduction:** Overproduced information in national security investigations must either be destroyed or returned to the USPS entity that produced it at the discretion of the field office or HQ division which requested the mail cover. If the information is returned, it must be accompanied with a letter to the USPS entity which produced the materials stating the reason(s) for the return of the information. If the information is to be destroyed, the supervisor responsible for the investigation must approve the destruction and its scope. This decision must be documented in an EC to the investigative file.

This Page is Intentionally Blank.

18.6.11 (U) INVESTIGATIVE METHOD: POLYGRAPH EXAMINATIONS

18.6.11.1 (U) SUMMARY

(U//FOUO) The polygraph examination is used in Predicated Investigations to: (i) aid in determining whether a person has pertinent knowledge of a particular matter under investigation or inquiry; (ii) aid in determining the truthfulness of statements made or information furnished by a subject, victim, witness, CHS, or an individual making allegations; and (iii) obtain information leading to the location of evidence, individuals or sites of offense.

(U//FOUO) Polygraphs are administered only to those who agree or volunteer to take the examination. An examination is conducted only when the examiner, in his/her professional judgment, believes the results will be accurate. All examinations must be conducted under an investigative file number.

(U//FOUO) This policy does not limit other authorized uses of polygraph method outside of Assessments or Predicated Investigations, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs.

18.6.11.2 (U) APPLICATION

(U//FOUO) This investigative method may be used in national security investigations, criminal investigations and positive foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. This method cannot be used during an Assessment, with the exception of Type 5 Assessments. See DIOG Section 5.6.3.4.8 and the IPG for the policy governing the use of polygraph examinations during a Type 5 Assessment.

18.6.11.3 (U) LEGAL AUTHORITY

(U) AGG-Dom, Part V.A.6.

18.6.11.4 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U//FOUO) An SSA may approve the use of a polygraph if:

- A) (U//FOUO) The individual agrees to or volunteers to take the examination;
- B) (U//FOUO) The examiner, in his/her professional judgment, believes the results will be accurate; and
- C) (U//FOUO) The investigative method is reasonably likely to achieve investigative objectives.

18.6.11.5 (U) DURATION OF APPROVAL

(U//FOUO) Polygraph examinations may be administered only to individuals who agree or volunteer to take an examination. The polygraph can be administered as long as the individual continues to agree to the examination, and the examiner, in his/her professional judgment,

believes the results will be accurate based upon an evaluation [assessment] of the physical and mental fitness of the examinee to undergo the examination.

18.6.11.6 (U) SPECIFIC PROCEDURES

(U//FOUO) An EC must be prepared requesting SSA approval for the polygraph. If an AUSA is assigned to the investigation, an FBI employee must confer with the USAO to discuss any prosecutorial issues prior to the administration of a polygraph.

18.6.11.7 (U) COMPLIANCE AND MONITORING

(U//FOUO) All polygraphs conducted in Predicated Investigations must be documented in the investigative file. Those polygraph examinations conducted in a Type 5 Assessment must be documented in the Assessment file.

18.6.12 (U) INVESTIGATIVE METHOD: TRASH COVERS (SEARCHES THAT DO NOT REQUIRE A WARRANT OR COURT ORDER)

18.6.12.1 (U) SUMMARY

(U) The Fourth Amendment to the United States Constitution prevents the FBI from conducting unreasonable searches and seizures. It also generally requires a warrant be obtained if the search will intrude on a reasonable expectation of privacy. To qualify as a “reasonable expectation of privacy,” the individual must have an actual subjective expectation of privacy and society must be prepared to recognize that expectation as objectively reasonable. See Katz v. United States, 389 U.S. at 361. If an individual has a reasonable expectation of privacy, a warrant or order issued by a court of competent jurisdiction or an exception to the requirement for such a warrant or order is required before a search may be conducted. Physical searches of personal or real property may be conducted without a search warrant or court order if there is no reasonable expectation of privacy in the property or area. As a general matter, there is no reasonable expectation of privacy in areas that are exposed to public view or that are otherwise available to the public.

(U//FOUO) **Note:** Consent Searches are authorized in Assessments, as well as in Predicated Investigations.

(U) A reasonable expectation of privacy may be terminated by an individual abandoning property, setting trash at the edge of the curtilage or beyond for collection, or when a private party reveals the contents of a package. However, the AGG-Dom and FBI policy have restricted the use of “trash covers” to Predicated Investigations as set forth in this section.

18.6.12.2 (U) APPLICATION

(U//FOUO) The FBI may conduct trash covers, as defined below in Section 18.6.12.4.1, in Predicated Investigations. This investigative method may be used in national security investigations, criminal investigations, foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3.

(U//FOUO) This method cannot be used during an Assessment, with the exception of a Type 5 Assessment. (See DIOG Section 5.6.3.4.8)

18.6.12.3 (U) LEGAL AUTHORITY

A) (U) AGG-Dom, Part V.A.3,

B) (U) Fourth Amendment to the United States Constitution

18.6.12.4 (U) DEFINITION OF INVESTIGATIVE METHOD

18.6.12.4.1 (U) DISTINCTION BETWEEN “TRASH COVERS” AND SEARCHES OF ABANDONED PROPERTY OR TRASH

A) (U//FOUO) **Trash Cover:** The intentional search of a specific person’s trash (that is located at the place for collection), whether from a home or business, designed to find information

relevant to an ongoing investigation when no reasonable expectation of privacy exists. A trash cover is a targeted effort to gather information regarding a particular person or entity by reviewing that person or entity's refuse. Generally, a trash cover is a planned in advance activity based upon information obtained that a specific trash container will contain evidence or intelligence of an investigative interest, and that such activity will occur over a specified period of time.

- B) (U//FOUO) **Search of Abandoned Property or Trash:** A search of abandoned property or trash that has been placed in a publicly accessible garbage container is not a "trash cover" under the definition above. If an FBI employee observes an individual abandoning something, for example, in a publicly accessible garbage can, or observes possible evidence of a crime or something of intelligence value in a public trash receptacle, the FBI employee may recover the item(s) without having an Assessment or Predicated Investigation open at that time.

18.6.12.4.2 (U) DETERMINATION OF AN AREA OF CURTILAGE AROUND A HOME

(U) Whether an area is curtilage around a home is determined by reference to four factors: (i) proximity of the area in question to the home; (ii) whether the area is within an enclosure surrounding the home; (iii) nature of the use to which the area is put; and (iv) steps taken to protect the area from observation by passers-by.

(U) An area is curtilage if it is so intimately tied to the home itself that it should be placed under the home's umbrella of Fourth Amendment protection.

18.6.12.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U//FOUO) SSA approval is required for the use of this method. However, if there is a doubt as to whether a person has a reasonable expectation of privacy in the area to be searched, the employee must consult with the CDC or OGC to determine whether a search warrant is required. Use of this method must be documented in the investigative file.

18.6.13 (U) INVESTIGATIVE METHOD: UNDERCOVER OPERATIONS

18.6.13.1 (U) SUMMARY

(U//FOUO) The undercover method of investigation, including use of proprietary business entities, is essential to the FBI's capability to covertly gather evidence and intelligence that will allow for the detection, disruption, prevention, and prosecution of individuals and enterprises that engage in criminal conduct or that pose a threat to the national security. The method inherently involves deception and may require cooperation with persons whose motivation and conduct are open to question. Accordingly, this method should be carefully considered and monitored throughout its use.

(U//FOUO) Undercover operations must be conducted in conformity with The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (AGG-UCO) in investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence. In investigations that concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the NSD in the review process. (AGG-Dom, Part V.A.7) Other undercover operations involving threats to the national security or foreign intelligence are reviewed and approved pursuant to FBI policy as described herein.

(U//FOUO) Application: This investigative method may be used in national security investigations, criminal investigations and positive foreign intelligence collection investigations, and for assistance to other agencies when it is not otherwise prohibited by AGG-Dom, Part III.B.2-3. This method cannot be used during an Assessment.

18.6.13.2 (U) LEGAL AUTHORITY

A) (U) AGG-Dom, Part V.A.7

B) (U) AGG-UCO

18.6.13.3 (U) DEFINITION OF INVESTIGATIVE METHOD

A) (U//FOUO) Undercover Activity: An "undercover activity" is any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function. An "undercover employee" is an employee of the FBI, another federal, state, or local law enforcement agency, another entity of the USIC, or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function.

B) (U//FOUO) Undercover Operation: An "undercover operation" is an operation that involves a series of related "undercover activities" over a period of time by an "undercover employee." A series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover activity involving sensitive circumstances, which are listed in the AGG-UCO and the FGUSO, constitutes an undercover operation regardless of the number of contacts involved. A substantive contact is a communication, whether by oral,

written, wire, or electronic means, that includes information of investigative interest. Mere incidental contact (e.g., a conversation that establishes an agreed time and location for another meeting) is not a substantive contact within the meaning of this policy.

18.6.13.3.1 (U) DISTINCTION BETWEEN SENSITIVE CIRCUMSTANCE AND SENSITIVE INVESTIGATIVE MATTER

(U//FOUO) The term “sensitive investigative matter” as used in the AGG-Dom should not be confused with the term “sensitive circumstance” as that term is used in undercover operations or ELSUR matters. The term sensitive circumstance relates to a circumstance that arises in an undercover operation that requires the UCO to obtain FBIHQ approval. A comprehensive list of sensitive circumstances for criminal activities is contained in the AGG-UCO and for national security matters in the National Security Undercover Operations Policy Implementation Guide (NSUCOPG). The Criminal Undercover Operations Review Committee (CUORC) and the national security Undercover Review Committee (UCRC) must review and approve undercover operations that involve sensitive circumstances. The detailed policy for undercover operations is described in this section of the DIOG, the Field Guide for Undercover and Sensitive Operations (FGUSO), the NSUCOPG, and the FBIHQ operational division PGs.

18.6.13.4 (U//FOUO) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

18.6.13.4.1 (U) STANDARDS FOR USE OF INVESTIGATIVE METHOD

(U//FOUO) An official considering approval or authorization of a proposed undercover application must weigh the risks and benefits of the operation, giving careful consideration to the following:

- A) (U//FOUO) The risks of personal injury to individuals, property damage, financial loss to persons or business, damage to reputation, or other harm to persons;
- B) (U//FOUO) The risk of civil liability or other loss to the government;
- C) (U//FOUO) The risk of invasion of privacy or interference with privileged or confidential relationships and any potential constitutional concerns or other legal concerns;
- D) (U//FOUO) The risk that individuals engaged in undercover operations may become involved in illegal conduct; and
- E) (U//FOUO) The suitability of government participation in the type of activity that is expected to occur during the operation. See AGG-UCO, Part IV.A.

18.6.13.4.2 (U//FOUO) APPROVAL REQUIREMENTS FOR UCOs (INVESTIGATIONS OF VIOLATIONS OF FEDERAL CRIMINAL LAW THAT DO NOT CONCERN THREATS TO NATIONAL SECURITY OR FOREIGN INTELLIGENCE)

(U//FOUO) The following approval and authorization requirements apply to undercover operations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence:

- A) (U//FOUO) An “undercover activity” in which an undercover employee plans to meet with a subject requires the approval of the SSA.
- B) (U//FOUO) An “undercover operation” must be approved by the SAC. The CDC must review all undercover operations before approval and provide advice to the SAC regarding predication of subjects, entrapment issues, and whether the proposal meets the requirements of the AGG-UCO or other DOJ and FBI policy guidance.
- C) (U//FOUO) In addition to SAC approval, authorization from the responsible FBIHQ Assistant Director or Executive Assistant Director must be obtained if the undercover operation involves a sensitive circumstance or certain fiscal circumstances, as those terms are defined in the AGG-UCO or other FBI guidance.
- D) (U//FOUO) Undercover operations that involve a sensitive circumstance (Group I undercover operations) require review by the CUORC as part of the authorization process. This requirement applies to both new and renewal proposals.
- E) (U//FOUO) Undercover operations that do not involve a sensitive circumstance (Group II undercover operations) require notice to the appropriate FBIHQ operational unit and to the Undercover and Sensitive Operations Unit following SAC approval. A renewal that would extend the operation beyond one year requires authorization from the responsible Assistant Director.
- F) (U//FOUO) All Innocent Images National Initiative (IINI) undercover operations deemed Group I and Group II operations require opening and renewal approvals from FBIHQ, Cyber Division. Group I IINI undercover operations will also be reviewed by the CUORC.
- G) (U//FOUO) Requirements for interim approval and emergency approval for undercover operations are contained in the FGUSO.

18.6.13.4.3 (U//FOUO) APPROVAL REQUIREMENTS FOR UCOS (INVESTIGATIONS OF VIOLATIONS THAT CONCERN THREATS TO NATIONAL SECURITY OR FOREIGN INTELLIGENCE)

(U//FOUO) The following approval requirements apply to undercover operations that concern threats to the national security or foreign intelligence:

- A) (U//FOUO) An “undercover operation” must be approved by the SAC. The CDC must review all undercover operations before approval and provide advice to the SAC regarding predication of subjects, entrapment issues, and whether the proposal meets the requirements of the NSUCOPG, or other DOJ and FBI policy guidance.
- B) (U//FOUO) In addition to SAC approval, authorization from the responsible FBIHQ Assistant Director or Executive Assistant Director must be obtained if the undercover operation involves a sensitive circumstance, as defined in NSUCOPG.
- C) (U//FOUO) Undercover operations that involve a sensitive circumstance must be reviewed and authorized by the responsible Assistant Director (Group I operations). Review by the UCRC must precede such authorization. If the matter involves religious or political organizations, the review must include participation by a representative of the DOJ NSD. See AGG-Dom, Section V; and NSUCOPG.
- D) (U//FOUO) Undercover operations that do not involve a sensitive circumstance (Group II undercover operations) must be forwarded to the appropriate operational unit at FBIHQ for review on a UACB basis prior to initiation of the operation. A renewal that would extend the operation beyond 12 months requires authorization from the responsible Deputy Assistant Director or Assistant Director.

- E) (U//FOUO) Requirements for interim approval and emergency approval for undercover operations are contained in NSUCOPG.

18.6.13.5 (U) DURATION OF APPROVAL

(U//FOUO) FBI undercover operations are generally approved for a maximum period of six months with six month renewal periods authorized thereafter.

18.6.13.6 (U) ADDITIONAL GUIDANCE

- A) (U//FOUO) The FGUSO provides additional guidance for the use of the undercover method in all undercover operations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence.
- B) (U//FOUO) Undercover activities and operations that concern threats to the national security or foreign intelligence must be carried out in conformity with the NSUCOPG and the appropriate investigative program PG that is responsible for the UCO.
- C) (U//FOUO) The FD-997, Application for Undercover Authority, must be used to obtain approvals for all undercover operations, Group I and Group II. Case agents should consult with the field office CDC and Undercover Coordinators in planning proposed UCOs.

18.6.13.7 (U) COMPLIANCE AND MONITORING, AND REPORTING REQUIREMENTS

(U//FOUO) All UCOs must provide an annual investigative/compliance summary using the FD-998 to appropriate FBIHQ undercover program managers.

18.7 (U) AUTHORIZED INVESTIGATIVE METHODS IN FULL INVESTIGATIONS

(U) See AGG-Dom, Part V.A.11-13.

(U) In Full Investigations, to include Enterprise Investigations, the authorized investigative methods include:

- A) (U) The investigative methods authorized for Assessments.
 - 1) (U) Public information. (See Section 18.5.1)
 - 2) (U) Records or information - FBI and DOJ. (See Section 18.5.2)
 - 3) (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (See Section 18.5.3)
 - 4) (U) On-line services and resources. (See Section 18.5.4)
 - 5) (U) CHS use and recruitment. (See Section 18.5.5)
 - 6) (U) Interview or request information from the public or private entities. (See Section 18.5.6)
 - 7) (U) Information voluntarily provided by governmental or private entities. (See Section 18.5.7)
 - 8) (U) Physical Surveillance (not requiring a court order). (See Section 18.5.8)
- B) (U) The investigative methods authorized for Preliminary Investigations.
 - 1) (U) Consensual monitoring of communications, including electronic communications. (See Section 18.6.1)
 - 2) (U) Intercepting the communications of a computer trespasser. (See Section 18.6.2)
 - 3) (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (See Section 18.6.3)
 - 4) (U) Administrative subpoenas. (See Section 18.6.4)
 - 5) (U) Grand jury subpoenas. (See Section 18.6.5)
 - 6) (U) National Security Letters. (See Section 18.6.6)
 - 7) (U) FISA Order for business records. (See Section 18.6.7)
 - 8) (U) Stored wire and electronic communications and transactional records. (See Section 18.6.8)¹⁸
 - 9) (U) Pen registers and trap/trace devices. (See Section 18.6.9)
 - 10) (U) Mail covers. (See Section 18.6.10)
 - 11) (U) Polygraph examinations. (See Section 18.6.11)
 - 12) (U) Trash Covers (Searches that do not require a warrant or court order). (See Section 18.6.12)
 - 13) (U) Undercover operations. (See Section 18.6.13)

¹⁸ (U//FOUO) The use of Search Warrants to obtain this information in Preliminary Investigations is prohibited. (See DIOG Section 18.6.8.4.2.3)

UNCLASSIFIED – FOR OFFICIAL USE ONLY

§18

Domestic Investigations and Operations Guide

C) (U) Searches – with a warrant or court order (reasonable expectation of privacy). (See Section 18.7.1 below)

D) (U) Electronic surveillance – Title III. (See Section 18.7.2 below)

E) (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (See Section 18.7.3 below)

(U//FOUO) Not all investigative methods are authorized while collecting foreign intelligence as part of a Full Investigation. See DIOG Section 9 for more information.

18.7.1 (U) INVESTIGATIVE METHOD: SEARCHES - WITH A WARRANT OR COURT ORDER (REASONABLE EXPECTATION OF PRIVACY)

(U) See AGG-Dom, Part V.A.12 and the Attorney General's Guidelines On Methods Of Obtaining Documentary Materials Held By Third Parties. Pursuant to Title II, Privacy Protection Act of 1980 (Pub. L. 96-440, Sec. 201 et seq.; 42 U.S.C. § 2000aa-11, et seq.).

18.7.1.1 (U) SUMMARY

(U) The Fourth Amendment to the United States Constitution governs all searches and seizures by government agents. The Fourth Amendment contains two clauses. The first establishes the prohibition against unreasonable searches and seizures. The second provides that no warrant (authorizing a search or seizure) will be issued unless based on probable cause. Although an unlawful search may not preclude a prosecution, it can have serious consequences for the government. These include adverse publicity, civil liability against the employee or the government and the suppression of evidence from the illegal seizure.

(U//FOUO) **Application:** Physical search requiring a judicial order or warrant may be used in a Full (national security and criminal) Investigation and to collect foreign intelligence information. This method may not be used for: (i) an Assessment or Preliminary Investigation; or (ii) providing assistance to other agencies, unless there is already an FBI FISA or warrant related to the request for assistance. Attorney General approval must be obtained prior to using any FISA-obtained or derived information in any proceeding whether foreign or domestic. When providing assistance to a foreign agency, information must be provided pursuant to the FBI Foreign Dissemination Manual and the FBI's Standard Minimization Procedures or other applicable minimization procedures."

(U) A search is a government invasion of a person's privacy. To qualify as reasonable expectation of privacy, the individual must have an actual subjective expectation of privacy and society must be prepared to recognize that expectation as objectively reasonable. See Katz v. United States, 389 U.S. at 361. The ability to conduct a physical search in an area or situation where an individual has a reasonable expectation of privacy requires a warrant or order issued by a court of competent jurisdiction or an exception to the requirement for such a warrant or order. The warrant or order must be based on probable cause. The United States Supreme Court defines probable cause to search as a "fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). A government agent may conduct a search without a warrant based on an individual's voluntary consent. A search based on exigent circumstances may also be conducted without a warrant, but the requirement for probable cause remains.

18.7.1.2 (U) LEGAL AUTHORITY

(U) Searches conducted by the FBI must be in conformity with FRCP Rule 41; FISA, 50 U.S.C. §§ 1821-1829; or E.O. 12333 § 2.5.

18.7.1.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) ***Physical Search defined:*** A physical search constitutes any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in the seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy.

(U) A physical search requiring a warrant does not include: (i) electronic surveillance as defined in FISA or Title III; or (ii) the acquisition by the United States Government of foreign intelligence information from international foreign communications, or foreign intelligence activities conducted according to otherwise applicable federal law involving a foreign electronic communications system, using a means other than electronic surveillance as defined in FISA.

18.7.1.3.1 (U) REQUIREMENT FOR REASONABLENESS

(U) By the terms of the Fourth Amendment, a search must be reasonable at its inception and reasonable in its execution. Whether a search meets Fourth Amendment standards will depend on the justification for the search and the scope of the search conducted. In all investigations, FBI employees must be prepared to articulate the basis for the search and the manner in which it was conducted.

18.7.1.3.2 (U) REASONABLE EXPECTATION OF PRIVACY

(U) The right of privacy is a personal right, not a property concept. It safeguards whatever an individual reasonably expects to be private. The protection normally includes persons, residences, vehicles, other personal property, private conversations, private papers and records. The Supreme Court has determined that there is no reasonable expectation of privacy in certain areas or information. As a result, government intrusions into those areas do not constitute a search and, thus, do not have to meet the requirements of the Fourth Amendment. These areas include: (i) open fields; (ii) prison cells; (iii) public access areas; and (iv) vehicle identification numbers. The Supreme Court has also determined that certain governmental practices do not involve an intrusion into a reasonable expectation of privacy and, therefore, do not amount to a search. These practices include: (i) aerial surveillance conducted from navigable airspace; (ii) field test of suspected controlled substance; and (iii) odor detection. A reasonable expectation of privacy may be terminated by an individual taking steps to voluntarily relinquish the expectation of privacy, such as abandoning property or setting trash at the edge of the curtilage or beyond for collection.

18.7.1.3.3 (U) ISSUANCE OF SEARCH WARRANT

(U) Under FRCP Rule 41, upon the request of a federal law enforcement officer or an attorney for the government, a search warrant may be issued by:

- A) (U) a federal magistrate judge, or if none is reasonably available, a judge of a state court of record within the federal district, for a search of property or for a person within the district;

- B) (U) a federal magistrate judge for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed;
- C) (U) a federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district, in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. § 2331); and
- D) (U) a magistrate with authority in the district to issue a warrant to install a tracking device. The warrant may authorize use of the device to track the movement of a person or property located within the district, outside, or both.

(U) Physical searches related to a national security purpose may be authorized by the FISC. (50 U.S.C. §§ 1821-1829)

18.7.1.3.4 (U) PROPERTY OR PERSONS THAT MAY BE SEIZED WITH A WARRANT

(U) A warrant may be issued to search for and seize any: (i) property that constitutes evidence of the commission of a criminal offense; (ii) contraband, the fruits of crime, or things otherwise criminally possessed; or (iii) property designed or intended for use or that is or has been used as the means of committing a criminal offense. In addition to a conventional search conducted following issuance of a warrant, examples of search warrants include:

18.7.1.3.4.1 (U) ANTICIPATORY WARRANTS

(U) As the name suggests, an anticipatory warrant differs from other search warrants in that it is not supported by probable cause to believe that contraband exists at the premises to be searched at the time the warrant is issued. Instead, an anticipatory search warrant is validly issued where there is probable cause to believe that a crime has been or is being committed, and that evidence of such crime will be found at the described location at the time of the search, but only after certain specified events transpire. These conditions precedent to the execution of an anticipatory warrant, sometimes referred to as "triggering events," are integral to its validity. Because probable cause for an anticipatory warrant is contingent on the occurrence of certain expected or "triggering" events, typically the future delivery, sale, or purchase of contraband, the judge making the probable cause determination must take into account the likelihood that the triggering event will occur on schedule and as predicted. Should these triggering events fail to materialize, the anticipatory warrant is void.

18.7.1.3.4.2 (U) SNEAK AND PEEK SEARCH WARRANTS

(U) A sneak and peek search warrant allows law enforcement agents to surreptitiously enter a location such as a building, an apartment, garage, storage shed, etc., for the purpose of looking for and documenting evidence of criminal activity. The purpose of this type of warrant is to search for and seize property (either tangible or intangible) without immediately providing notice of the search and a return on the warrant to the owner of the property searched or seized. See FRCP 41(f)(3). A sneak and peek warrant is used to gather additional evidence of criminal activity without prematurely exposing an

on-going investigation. The evidence discovered during a sneak and peek search may be used to support a request for a conventional search warrant.

18.7.1.3.4.3 (U) MAIL OPENINGS

(U) Mail in United States postal channels may be searched only pursuant to court order, or presidential authorization. United States Postal Service regulations governing such activities must be followed. A search of items that are being handled by individual couriers, or commercial courier companies, under circumstances in which there is a reasonable expectation of privacy, or have been sealed for deposit into postal channels, and that are discovered within properties or premises being searched, must be carried out according to unconsented FISA or FRCP Rule 41 physical search procedures.

18.7.1.3.4.4 (U) COMPELLED DISCLOSURE OF THE CONTENTS OF STORED WIRE OR ELECTRONIC COMMUNICATIONS

(U) Contents in "electronic storage" (e.g., unopened e-mail/voice mail) require a search warrant. See 18 U.S.C. § 2703(a). A distinction is made between the contents of communications that are in electronic storage (e.g., unopened e-mail) for less than 180 days and those in "electronic storage" for longer than 180 days, or those that are no longer in "electronic storage" (e.g., opened e-mail). In enacting the ECPA, Congress concluded that customers may not retain a "reasonable expectation of privacy" in information sent to network providers. However, the contents of an e-mail message that is unopened should nonetheless be protected by Fourth Amendment standards, similar to the contents of a regularly mailed letter. On the other hand, if the contents of an unopened message are kept beyond six months or stored on behalf of the customer after the e-mail has been received or opened, it should be treated the same as a business record in the hands of a third party, such as an accountant or attorney. In that case, the government may subpoena the records from the third party without running afoul of either the Fourth or Fifth Amendment. If a search warrant is used, it may be served on the provider without notice to the customer or subscriber.

18.7.1.3.4.4.1 (U) SEARCH WARRANT

(U/FOUO) Investigators can obtain the full contents of a network account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant. Warrants issued under 18 U.S.C. § 2703 must either comply with FRCP Rule 41 or be an equivalent state warrant. Warrants issued pursuant to 18 U.S.C. § 2703 do not require personal service on the customer; the warrants are only be served on the electronic communication service or a remote computing service. FRCP Rule 41 requires a copy of the warrant be left with the provider, and a return and inventory be made. Federal courts have nationwide jurisdiction to issue these search warrants (see below).

(U) With a search warrant issued based on probable cause pursuant to FRCP Rule 41 or an equivalent state warrant, the government may obtain:

A) (U) The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for one hundred and eighty days or less, and

B) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order with notice.

(U) In other words, every record and all of the stored contents of an account—including opened and unopened e-mail/voice mail— can be obtained with a search warrant based on probable cause pursuant to FRCP Rule 41. Moreover, because the warrant is issued by a neutral magistrate based on a finding of probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

18.7.1.3.4.4.2 (U) NATIONWIDE SCOPE

(U) Search warrants under 18 U.S.C. § 2703(a) may be issued by a federal "court with jurisdiction over the offense under investigation," and may be executed outside the district of the issuing court for material responsive to the warrant. State courts may also issue warrants under 18 U.S.C. § 2703(a), but the statute does not give these warrants effect outside the issuing court's territorial jurisdiction. As with any other FRCP Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with FRCP Rule 41.

18.7.1.3.4.4.3 (U) SERVICE OF PROCESS

(U) 18 U.S.C. § 2703(a) search warrants are obtained just like any other FRCP Rule 41 search warrant but are typically served on the provider and compel the provider to find and produce the information described in the warrant. ECPA expressly states that the presence of an officer is not required for service or execution of a search warrant issued pursuant to 18 U.S.C. § 2703(a).

18.7.1.3.4.4.4 (U) COURT ORDER WITH PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U//FOUO) Investigators can obtain everything in a network account except for unopened e-mail or voice-mail stored with a provider for 180 days or less using a 18 U.S.C. § 2703(d) court order with prior notice to the subscriber unless they have obtained authority for delayed notice pursuant to 18 U.S.C. § 2705. ECPA distinguishes between the contents of communications that are in "electronic storage" (e.g., unopened e-mail) for less than 180 days, and those that have been in "electronic storage" for longer or that are no longer in "electronic storage" (e.g., opened e-mail).

(U) FBI employees who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a), may obtain:

A) (U) "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

B) (U) "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. §§ 2703(b)(1)(B)(ii), 2703 (b)(2); and

C) (U) Everything that can be obtained using a 18 U.S.C. § 2703(d) court order without notice.

(U) As a practical matter, this means that the government can obtain all associated subscriber and transactional records and the full contents of a subscriber's account except unopened e-mail and voicemail (that has been in "electronic storage" 180 days or less) using a 18 U.S.C. § 2703(d) order that complies with the prior notice provisions of 18 U.S.C. § 2703(b)(1)(B).

(U) If notice would jeopardize the investigation, FBI employees can obtain an order delaying notice for up to ninety days. See 18 U.S.C. § 2705(a). A request to delay notice may be included in the 18 U.S.C. § 2703(d) application and proposed order. FBI employees may also apply to the court for extensions of the delay. See 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(4). Upon expiration of the delayed notice period, the government is required to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5).

18.7.1.3.4.4.5 (U) LEGAL STANDARD

(U) To order delayed notice, the court must find that "there is reason to believe that notification of the existence of the court order may... endanger the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A) and 2705(a)(2). The applicant must satisfy this standard anew each time an extension of the delayed notice is sought.

18.7.1.3.4.4.6 (U) NATIONWIDE SCOPE

(U) Federal court orders under 18 U.S.C. § 2703(d) have effect outside the district of the issuing court. Orders issued pursuant to 18 U.S.C. § 2703(d) may compel providers to disclose information even if the information is stored outside the district of the issuing court. See 18 U.S.C. § 2703(d) ("any court that is a court of competent jurisdiction" may issue a 18 U.S.C. § 2703[d] order); 18 U.S.C. § 2711(3) (court of competent jurisdiction includes any federal court having jurisdiction over the offense being investigated without geographic limitation).

(U) 18 U.S.C. § 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B). Such orders issued by state courts, however, do not have effect outside the jurisdiction of the issuing state. See 18 U.S.C. §§ 2711(3).

18.7.1.3.4.4.7 (U) COURT ORDER WITHOUT PRIOR NOTICE TO THE SUBSCRIBER OR CUSTOMER

(U) A court order under 18 U.S.C. § 2703(d) may compel disclosure of:

- A) (U) All "record(s) or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])," and
- B) (U) Basic subscriber information that can be obtained using a subpoena without notice. 18 U.S.C. § 2703(c)(1).

18.7.1.4 (U) APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

- A) (U//FOUO) **Search warrants issued under authority of FRCP Rule 41:** A warrant to search is issued by a federal magistrate (or a state court judge if a federal magistrate is not reasonably available). Coordination with the USAO or DOJ is required to obtain the warrant.
- B) (U//FOUO) **FISA:** In national security investigations, field office requests for FISA authorized physical searches must be submitted to FBIHQ using the FBI FISA Request Form. Field office requests for FISA approval are tracked through FISAMS. This form should be completed by the case agent.
- C) (U//FOUO) **Sensitive Investigative Matters (SIM):** Notice to the appropriate FBIHQ operational Unit Chief and Section Chief is required if the matter under investigation is a sensitive investigative matter. Notice to DOJ is also required, as described in DIOG Section 10.

18.7.1.5 (U) DURATION OF APPROVAL

(U) The duration for the execution of a warrant is established by the court order or warrant.

18.7.1.6 (U) SPECIFIC PROCEDURES

18.7.1.6.1 (U) OBTAINING A WARRANT UNDER FRCP RULE 41

18.7.1.6.1.1 (U) PROBABLE CAUSE

(U//FOUO) After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under FRCP Rule 41(c). Probable cause exists where "the facts and circumstances within the FBI employee's knowledge, and of which they had reasonably trustworthy information are sufficient in themselves to warrant a person of reasonable caution in the belief that..." a crime has been or is being committed, and that sizable property can be found at the place or on the person to be searched. Probable cause is a reasonable belief grounded on facts. In judging whether a reasonable belief exists, the test is whether such a belief would be engendered in a prudent person with the officer's training and experience. To establish probable cause, the affiant must demonstrate a basis for knowledge and belief that the facts are true and that there is probable cause to believe the items listed in the affidavit will be found at the place to be searched.

18.7.1.6.1.2 (U) REQUESTING A WARRANT IN THE PRESENCE OF A JUDGE

- A) (U) **Warrant on an Affidavit:** When a federal law enforcement officer or an attorney for the government presents an affidavit in support of a warrant, the judge may require the affiant to

appear personally and may examine under oath the affiant and any witness the affiant produces.

- B) (U) **Warrant on Sworn Testimony**: The judge may wholly or partially dispense with a written affidavit and base a warrant on sworn testimony if doing so is reasonable under the circumstances.
- C) (U) **Recording Testimony**: Testimony taken in support of a warrant must be recorded by a court reporter or by a suitable recording device, and the judge must file the transcript or recording with the clerk, along with any affidavit.

18.7.1.6.1.3 (U) REQUESTING A WARRANT BY TELEPHONIC OR OTHER MEANS

- A) (U) **In General**: A magistrate judge may issue a warrant based on information communicated by telephone or other appropriate means, including facsimile transmission.
- B) (U) **Recording Testimony**: Upon learning that an applicant is requesting a warrant, a magistrate judge must: (i) place under oath the applicant and any person on whose testimony the application is based; and (ii) make a verbatim record of the conversation with a suitable recording device, if available, or by a court reporter, or in writing.
- C) (U) **Certifying Testimony**: The magistrate judge must have any recording or court reporter's notes transcribed, certify the transcription's accuracy, and file a copy of the record and the transcription with the clerk. Any written verbatim record must be signed by the magistrate judge and filed with the clerk.
- D) (U) **Suppression Limited**: Absent a finding of bad faith, evidence obtained from a warrant issued under FRCP Rule 41(d)(3)(A) is not subject to suppression on the ground that issuing the warrant in that manner was unreasonable under the circumstances.

18.7.1.6.1.4 (U) ISSUING THE WARRANT

(U) In general, the magistrate judge or a judge of a state court of record must issue the warrant to an officer authorized to execute it. The warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 10 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant.

18.7.1.6.1.5 (U) WARRANT BY TELEPHONIC OR OTHER MEANS

- (U) If a magistrate judge decides to proceed under FRCP Rule 41(d)(3)(A), the following additional procedures apply:
 - A) (U) **Preparing a Proposed Duplicate Original Warrant**: The applicant must prepare a "proposed duplicate original warrant" and must read or otherwise transmit the contents of that document verbatim to the magistrate judge.
 - B) (U) **Preparing an Original Warrant**: The magistrate judge must enter the contents of the proposed duplicate original warrant into an original warrant.

- C) (U) **Modifications:** The magistrate judge may direct the applicant to modify the proposed duplicate original warrant. In that case, the judge must also modify the original warrant.
- D) (U) **Signing the Original Warrant and the Duplicate Original Warrant:** Upon determining to issue the warrant, the magistrate judge must immediately sign the original warrant, enter on its face the exact time it is issued, and direct the applicant to sign the judge's name on the duplicate original warrant.

18.7.1.6.1.6 (U) EXECUTING AND RETURNING THE WARRANT

- A) (U) **Noting the Time:** The officer executing the warrant must enter on its face the exact date and time it is executed.
- B) (U) **Inventory:** An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person.
- C) (U) **Receipt:** The officer executing the warrant must: (i) give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken; or (ii) leave a copy of the warrant and receipt at the place where the officer took the property.
- D) (U) **Return:** The officer executing the warrant must promptly return it — together with a copy of the inventory — to the magistrate judge designated on the warrant. The judge must, on request, give a copy of the inventory to the person from whom, or from whose premises, the property was taken and to the applicant for the warrant.

18.7.1.6.1.7 (U) FORWARDING PAPERS TO THE CLERK

(U) The magistrate judge to whom the warrant is returned must attach to the warrant a copy of the return, the inventory, and all other related papers and must deliver them to the clerk in the district where the property was seized. (FRCP Rule 41)

18.7.1.6.1.8 (U) WARRANT FOR A TRACKING DEVICE

- A) (U) **Noting the Time:** The officer executing a tracking device warrant must enter on it the exact date and time the device was installed and the period during which it was used.
- B) (U) **Return:** Within 10 calendar days after the use of the tracking device has ended, the officer executing the warrant must return it to the judge designated in the warrant.
- C) (U) **Service:** Within 10 calendar days after use of the tracking device has ended, the officer executing the warrant must serve a copy of the warrant on the person who was tracked. Service may be accomplished by delivering a copy to the person who, or whose property was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address. Upon request of the government, the judge may delay notice as provided in FRCP Rule 41(f)(3).

18.7.1.6.1.9 (U) DELAYED NOTICE

(U) Upon the government's request, a magistrate judge—or if authorized by FRCP Rule 41(b), a judge of a state court of record—may delay any notice required by FRCP Rule 41 if the delay is authorized by statute.

18.7.1.6.2 (U) OBTAINING A FISA WARRANT

(U) Applications for court-authorized physical search pursuant to FISA must be made by a federal officer in writing upon oath or affirmation and with the specific approval of the Attorney General. (See 50 U.S.C. § 1823).

18.7.1.6.2.1 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

(U) Each FISA application must be accompanied by a Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that: the information being sought is foreign intelligence information; that a significant purpose of the search is to obtain foreign intelligence information; that such information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.

(U) 50 U.S.C. § 1823 specifies the Assistant to the President for National Security Affairs; E.O. 12139 as amended by E.O. 13383 specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA. The FBI Director has represented to Congress that the FBI deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.1.6.2.2 (U) LENGTH OF PERIOD OF AUTHORIZATION FOR FISC ORDERS

(U) Generally, a FISC Order approving an unconsented physical search will specify the period of time during which physical searches are approved and provide that the government will be permitted the period of time necessary to achieve the purpose, or for 90 days, whichever is less, except that authority may be:

- A) (U) For no more than one year for "Foreign Power" targets (establishments); or
- B) (U) For no more than 120 days for a non-USPER agent of a foreign power, with renewals for up to one.

18.7.1.6.2.3 (U) EXTENSION OF PHYSICAL SEARCH AUTHORITY

(U//FOUO) An extension of physical search authority may be granted on the same basis as the original order upon a separate application for an extension and upon new findings made in the same manner as the original order.

18.7.1.6.2.4 (U) EMERGENCY FISA AUTHORITY

- A) (U) The Attorney General may authorize an emergency physical search under FISA when he reasonably makes a determination that an emergency situation exists that precludes advance FISA court review and approval, and there exists a factual predication for the issuance of a FISA Court Order. In such instances, a FISC judge must be informed by the Attorney General or his designee at the time of the authorization and an application according to FISA requirements is submitted to the judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General.
- B) (U) If a court order is denied after an emergency authorization has been initiated, no information gathered as a result of the search may be used in any manner except if with the approval of the Attorney General, the information indicates a threat of death or serious bodily harm to any person.
- C) (U//FOUO) For an emergency FISA for physical search, DOJ OI can be reached during regular business hours at (202) 514-5600 or through secure or through the DOJ Command Center at (202) 514-5000 at any time.

18.7.1.6.2.5 (U) SPECIAL CIRCUMSTANCES

(U) The President through the Attorney General may also authorize a physical search under FISA without a court order for periods of up to one year, if the Attorney General certifies that the search will be solely directed at premises, information, material, or property that is used exclusively by or under the open and exclusive control of a foreign power; there is no substantial likelihood that the physical search will involve the premises, information, material, or property of a United States person; and there are minimization procedures that have been reported to the court and Congress. The FBI's involvement in such approvals is usually in furtherance of activities pursued according to E.O. 12333. Copies of such certifications are to be transmitted to the FISA Court. See 50 U.S.C. § 1822[a].

(U) Information concerning USPERs acquired through unconsented physical searches may only be used according to minimization procedures. See: 50 U.S.C. §§ 1824(d)(4) and 1825(a).

18.7.1.6.2.6 (U) REQUIRED NOTICE

(U) If an authorized search involves the premises of an USPER, and the Attorney General determines that there is no national security interest in continuing the secrecy of the search, the Attorney General must provide notice to the USPER that the premises was searched and the identification of any property seized, altered, or reproduced during the search.

18.7.1.6.2.7 (U//FOUO) FISA VERIFICATION OF ACCURACY PROCEDURES

(U//FOUO) The accuracy of information contained within FISA applications is of utmost importance and must be reviewed in accordance with the FISA Accuracy Policy Implementation Guide.

(U//FOUO) Only documented and verified information may be used to support FBI applications to the court. In addition to the certifications required through FISAMS, the following administrative procedures must be followed for every FISA application:

- A) (U//FOUO) Each investigative file for which an application is prepared for submission to the FISC must include a FISA Accuracy sub-file. This sub-file must be used for copies of all of the supporting documentation relied upon when making the certifications contained on the FISA Verification Form (“Woods Form”), which is available in the Forms section of the NSLB library at <http://home.fbinet.fbi/DO/OGC/Main%20Law%20Library/Forms/NSLB%20Library.aspx>. A FISA accuracy sub-file must include:
- 1) (U//FOUO) FBI database checks that were conducted to determine whether the target of the proposed FISA is also the subject of an FBI criminal investigation, past or present;
 - 2) (U//FOUO) CHS file checks (DELTA, 134, 137, 270, and 307 files) that were conducted to determine whether the target has, or has had, a relationship with the FBI as a CHS; and
 - 3) (U//FOUO) Copies of the most authoritative documents that exist for each fact asserted in the application. The most authoritative document may be a cable, EC, letterhead memorandum (LHM), FISA intercept (“tech cut”), etc. The agent must use some judgment in ascertaining appropriate documentation, but, in general, the agent should attempt to get as close as possible to original documentation of a fact. For example, if the target’s immigration status is summarized in an EC, the agent should strive to obtain a copy of the underlying immigration document to verify the fact(s) asserted rather than relying on the EC. Similarly, if the application states that a National Security Letter (NSL) was served on a certain date, there should be a copy of the NSL in the subfile instead of the EC that states an NSL was served. For more guidance on this issue, see FISA Accuracy PG at: <http://home/forms/fd1028/Policy%20and%20Guidance%20Library/0394PG.pdf>
- B) (U//FOUO) Every FISA application is subject to review through two oversight mechanisms designed to ensure that FBI field offices take appropriate steps regarding the factual accuracy of statements to the FISC. First, CDCs in the field are required to conduct accuracy reviews of limited numbers of FISAs in accordance with procedures established by the General Counsel. Second, OI attorneys conduct accuracy reviews with CDC and NSLB participation on approximately an annual basis. A full description of each of these reviews can be found in the FISA Accuracy PG at: <http://home/forms/fd1028/Policy%20and%20Guidance%20Library/0394PG.pdf>

18.7.1.6.2.8 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone “who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . .” See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG’s Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that use authority be obtained for foreign proceedings as well. Questions concerning the FISA use policy or

requests for assistance in obtaining FISA use authority from the AG should be directed to NSLB's Classified Litigation Support Unit.

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the "aggrieved person" [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.7.1.6.2.9 (U//FOUO) FISA PHYSICAL SEARCH ADMINISTRATIVE SUB-FILE

(U//FOUO) Each investigative file for which an application is or has been prepared for submission to the FISC will include a sub-file to be labeled FISA Physical Search Administration Sub-File. This sub-file is to contain copies of all applications to and orders issued by the FISC for the conduct of physical searches in the investigation. The following data must be included in this FISA Physical Search Administrative Sub-file:

- A) (U//FOUO) The identities of the persons or entities that are the subject of the physical search; and
- B) (U//FOUO) The description of the premises or property that is the subject of the physical search.

18.7.1.6.2.10 (U//FOUO) FISA RENEWALS

(U//FOUO) A FISA Review Board has been established that is responsible for reviewing, on a monthly basis, those FISAs (other than certain FISAs from the Counterintelligence Division), that have been maintained for more than one year. The FISA Review Board meeting schedule and required justifications for requests for continued renewal are contained and processed through FISAMS.

(U//FOUO) The Board assesses the quality and quantity of foreign intelligence that has been generated by the FISA; the continued need for the foreign intelligence that is being generated by the coverage; the strategy and timing of any criminal prosecution that might be contemplated against the target; any backlog in translation of the results of the surveillance; and the relative risk to national security if the FISA is not renewed.

(U//FOUO) The Board will provide an explanation of the reason for denying permission to renew a FISA. If there is a dissenting opinion, the request to renew and the Board's position will be forwarded to the EAD NSB for an expeditious review. The Review Board's decision on renewals with dissenting opinions will be final, unless overruled by the EAD NSB.

18.7.1.6.2.10.1 (U) APPEALING THE DECISION OF THE REVIEW BOARD

(U//FOUO) Should the field office responsible for a FISA disagree with the decision of the Board, the field office may present his or her position, by EC, to the Assistant Director (AD) responsible for the FISA. The AD will consider the merits of any additional information not previously submitted in writing to the Board and may choose

to present a written appeal (EC) for further consideration to the EAD NSB. An EC documenting the decision of the EAD must be provided to the field office promptly upon the EAD's NSB final decision.

18.7.1.6.2.11 (U) COMPLIANCE AND MONITORING FOR FISA

(U//FOUO) All compliance issues related to FISA physical search must be reported to the Unit Chief of OGC National Security Law Policy and Training Unit, or successor position (soon to be renamed the OGC National Security Law Compliance, Oversight, and Training Unit).

18.7.1.6.2.12 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization ("FISA overcollection") will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.7.2 (U) INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – TITLE III

18.7.2.1 (U) SUMMARY

(U//FOUO) Electronic Surveillance (ELSUR) under Title III is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's law enforcement. To ensure that due consideration is given to the competing interests between law enforcement and the effect on privacy and civil liberties, this section contains various administrative and management controls beyond those imposed by statute and DOJ guidelines. Unless otherwise noted, it is the responsibility of the case agent and his/her supervisor to ensure compliance with these instructions. Title III ELSUR is only authorized as an investigative method in the conduct of Full Investigations. Title III ELSUR requires: (i) administrative or judicial authorization prior to its use; (ii) contact with the field office ELSUR Technician to coordinate all necessary recordkeeping; and (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U//FOUO) **Application:** Title III ELSUR may be used in a Full (criminal) Investigation. This method may not be used for: (i) an Assessment or Preliminary Investigation; or (ii) providing assistance to other agencies, unless there is already an FBI Title III related to the request for assistance. When providing assistance to a foreign agency, information must be provided pursuant to the FBI's Foreign Dissemination Manual.

18.7.2.2 (U) LEGAL AUTHORITY

(U) Title III ELSUR is authorized by chapter 119, 18 U.S.C. §§ 2510-2522 (Title III of the Omnibus and Safe Streets Act of 1968).

18.7.2.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Title III ELSUR is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

18.7.2.4 (U) TITLE III GENERALLY

(U) With the prior approval of the Attorney General, or Attorney General's designee, the United States Attorney, by and through an AUSA, or the Strike Force Attorney, may apply to a federal judge for a court order authorizing the interception of wire, oral, or electronic communications relating to one or more of the offenses listed in Title III (18 U.S.C. § 2516). Judicial oversight continues throughout the operational phase of the electronic surveillance including the installation, monitoring, and handling of recording media.

(U) For purposes of obtaining review and approval for use of the method, Title III applications are considered to be either "sensitive" or "non-sensitive." The requirements for each are set forth below.

18.7.2.5 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR NON-SENSITIVE TITLE IIIs

(U//FOUO) An SAC is the authorizing official to approve all requests for “non-sensitive” Title III orders, including original, extension, and renewal applications. SAC approval of all extensions and renewals is required to ensure that field office managers will allocate the resources necessary to use this method. Any delegation of SAC approval authority to an ASAC under this section must be in writing.

(U//FOUO) Prior to SAC approval referred to above, CDC or OGC review is required for the initial “non-sensitive” Title III order. Extensions and renewals sought within 30 days after the expiration of the original Title III order in non-sensitive Title IIIs do not require CDC review, unless requested by the SAC or designee. The CDC must review renewals sought more than 30 days after the expiration of the original Title III order.

(U//FOUO) There may be situations or unusual circumstances requiring the FBI to adopt an already existing Title III from another federal law enforcement agency. Such adoptions may only be done on a case-by-case basis, in exceptional circumstances, and subject to the requirements set forth herein relating to CDC review and SAC approval. Should the Title III proposed for adoption involve sensitive circumstances, it must also be handled in accordance with the approval and review requirements set forth below.

18.7.2.6 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR SENSITIVE TITLE IIIs

(U//FOUO) All Title III applications involving one of the seven “sensitive circumstances,” listed below, including all extensions and renewals, must be reviewed by OGC and approved by FBIHQ. The SAC, with the recommendation of the CDC, must determine whether the request involves sensitive circumstances. The term “sensitive circumstances” as used in this section relating to electronic surveillance under Title III is different from the term “sensitive investigative matters,” as used in conjunction with approval requirements for opening Assessments and Predicated Investigations, and is different from the term “sensitive monitoring circumstances” as used in conjunction with the approval requirements for consensual monitoring.

(U//FOUO) The field office must include a copy of the completed CDC checklist (FD-926) when forwarding the initial sensitive Title III applications to OGC and FBIHQ for review. After the initial submission, the CDC checklist must be completed by the appropriate OGC unit for all subsequent extensions or renewals of sensitive Title IIIs.

(U//FOUO) Although ultimate approval for sensitive Title IIIs is at the FBIHQ level, the SAC or ASAC must continue to review and approve the use of the method for all sensitive Title III applications as it relates to the allocation of resources within their field office.

(U//FOUO) The following five sensitive circumstances require the approval of a Deputy Assistant Director (DAD) or a higher level official from the Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD), as appropriate:

- A) (U//FOUO) Significant privilege issues or First Amendment concerns (e.g., attorney-client privilege or other privileged conversations or interception of news media representatives);
- B) (U//FOUO) Significant privacy concerns are anticipated (e.g., placing a microphone in a bedroom or bathroom);
- C) (U//FOUO) Application is based on “relaxed specificity” (i.e., “roving” interception) under 18 U.S.C. § 2518(11)(a) and (b);
- D) (U//FOUO) Application concerns a Domestic Terrorism (DT), International Terrorism, or Espionage investigation; or
- E) (U//FOUO) Any situation deemed appropriate by the AD of CID or OGC.

(U//FOUO) The following two sensitive circumstances require the approval of the Director, the Acting Director, Deputy Director, or the Executive Assistant Director (EAD) for the Criminal Cyber Response and Services Branch or National Security Branch, or the respective Assistant Director for Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Weapons of Mass Destruction Directorate (WMDD), or Counterintelligence Division (CD):

- A) (U//FOUO) “Emergency” Title III interceptions (i.e., interceptions conducted prior to judicial approval under 18 U.S.C. § 2518(7)); or
- B) (U//FOUO) It is anticipated that conversations of members of Congress, federal judges, high-level federal officials, high-level state executives, or members of a state judiciary or legislature will be intercepted.

(U//FOUO) “Sensitive circumstances” may develop at any point in time during the course of a Title III. For example, while an initial application for interceptions might not be considered sensitive, conversations intercepted thereafter of a high-level state executive would render any subsequent spinoffs, extensions, or renewals “sensitive” Title III requests.

18.7.2.7 (U) PROCEDURES FOR EMERGENCY TITLE III INTERCEPTIONS

(U//FOUO) 18 U.S.C. § 2518(7) provides that any investigative or law enforcement officer, specially designated by the Attorney General, Deputy Attorney General, or the Associate Attorney General, who reasonably determines that an emergency situation exists that requires communications to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and there are grounds upon which an order could be entered authorizing interception, may intercept such communications.

(U//FOUO) Section 2518(7) postpones, rather than eliminates the need for judicial authorization. If the Attorney General, Deputy Attorney General, or the Associate Attorney General authorizes an appropriate FBI official to approve an emergency Title III interception, an after-the-fact application for an order approving the interception must be made in accordance with Title III to the appropriate Court, and an order obtained, within 48 hours after the interception has occurred or begins to occur.

(U//FOUO) All emergency interceptions must be coordinated with the Department of Justice, Office of Enforcement Operations (DOJ/OEO). No SAC or FBIHQ official has the authority on his/her own to authorize interception of wire, oral, or electronic communications, even under emergency circumstances and/or where a human life is in jeopardy. The use of

emergency Title III interceptions is a “sensitive circumstance” requiring the approval of the Director, Deputy Director, EAD for the Criminal Cyber Response and Services Branch, EAD for the National Security Branch, or the respective Assistant Director for Criminal Investigative Division (CID), Cyber Division, Counterterrorism Division (CTD), Counterintelligence Division (CD), or Weapons of Mass Destruction Directorate (WMDD). See DIOG Section 18.7.2.2.

(U) 18 U.S.C. § 2518(7) defines an emergency situation as one involving:

- A) (U) immediate danger of death or serious physical injury to any person.
- B) (U) conspiratorial activities threatening the national security interest, or
- C) (U) conspiratorial activities characteristic of organized crime.

(U//FOUO) In all but the most unusual circumstances, the only situations likely to constitute an emergency by the Department of Justice (DOJ) are those involving an imminent threat to life, e.g., a kidnapping, hostage taking, or imminent terrorist activity.

18.7.2.7.1 (U) OBTAINING EMERGENCY AUTHORIZATION

(U//FOUO) Should a situation arise requiring emergency Title III authority, the field office, with the approval of the SAC, should do the following:

- A) (U//FOUO) Notify the appropriate United States Attorney’s Office (USAO) to coordinate the determination of whether the facts and circumstances meet the requirements of 18 U.S.C. § 2518(7). Generally, the AUSA will contact the DOJ OEO, which will initiate and coordinate the approval process for DOJ authorization. Should an AUSA not be readily available, the field office should contact OGC, which will contact OEO directly. For emergency Title III requests involving Criminal, DT, WMD, or Cyber matters, contact should be made with the Unit Chief, Investigative Law Unit, ILTB. For emergency Title III requests involving Counterintelligence matters, contact should be made with the Unit Chief, Counterintelligence Law Unit, NSLB. For emergency Title III requests involving international terrorism matters, contact should be made with the Unit Chief, Counterterrorism Law Unit I or II, NSLB. Should contact be made directly between the FBI and OEO, the appropriate United States Attorney’s Office should be notified as soon thereafter as possible.
- B) (U//FOUO) Telephonically advise the appropriate operational unit at FBIHQ of the emergency request and immediately submit a written Request for Emergency Title III, either via facsimile or via email as an attachment. A sample Request for Emergency Title III form is located in DIOG Appendix H. The Request for Emergency Title III should be filled out by the case agent or another law enforcement officer familiar with the specific facts of the investigation and shall include a concise written statement of the facts, circumstances, and probable cause supporting the request for interception, as well as an indication of the nature of the emergency (i.e., immediate danger of death or serious physical injury to any person). The operational FBIHQ unit will then convey the facts and circumstances supporting the request to OGC to determine whether the statutory requirements for an emergency and probable cause for an interception exist. If emergency authority is determined to be appropriate, the operational unit will then take the steps necessary to present the request to the Director, or his designee for approval.
- C) (U//FOUO) During off-duty hours, requesting field offices should direct emergency Title III requests to the FBI’s Strategic Information and Operations Center (SIOC), which will contact:

the appropriate operational unit. Unless time does not permit, OGC concurrence should be obtained during off-duty hours as well.

D) (U//FOUO) Notify the TA and the TTA to coordinate technical equipment requirements.

(U//FOUO) While the FBIHQ operational unit is processing the emergency Title III request for approval, OEO will be doing the same. If DOJ agrees to the request, OEO will contact FBIHQ and the AUSA to advise it of that fact. The Director, or his designee will then contact the AG or his designee personally and request authorization to make the final probable cause determination and to authorize electronic surveillance pursuant to 18 U.S.C. § 2518(7). The Director, Acting Director, or his designee will then notify the operational unit of the exact time the AG or his designee granted authority to proceed. The individual in the operational unit at FBIHQ who receives the information regarding the AG authority to proceed must note the exact time of the authorization on the "Emergency Electronic Surveillance Authorization Verification Form." The form is at: Emergency Electronic Surveillance Authorization Verification. The operational unit must then contact OEO and relay this information. OEO is responsible for recontacting the AUSA to advise him/her when the 48-hour period began.

18.7.2.7.2 (U) POST-EMERGENCY AUTHORIZATION

(U//FOUO) Once the AG or his designee has authorized the Director, or his designee to make the determination whether to proceed with the emergency Title III, the government has 48 hours (including weekends and holidays) from the time the AG granted authorization to apply for a court order approving the interception. The field office, in coordination with the AUSA, must immediately begin preparing an affidavit, application and proposed order for court authorization.

(U//FOUO) The affidavit in support of the after-the-fact application to the court for an order approving the emergency interception must contain only those facts known to the AG or his designee at the time the emergency interception was approved. The application must be accompanied by the "Emergency Electronic Surveillance Authorization Verification" form, which must reflect the date and time of the emergency authorization.

(U//FOUO) The government may also request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial 48 hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of both requests. However, the affidavit must clearly indicate what information was communicated to the AG or his designee at the time the emergency interception was approved and what information was developed thereafter. Two separate applications and proposed orders should be submitted to the court in this situation – one set for the emergency and one set for the extension. If continued interceptions are not being sought, no further authorization is needed from OEO. The AUSA should, however, still submit the application, affidavit, and order to OEO for review. If continued interceptions are sought, that application, affidavit, and order must be reviewed by OEO and approved by DOJ like any other Title III request. In either situation, the affidavit must also be submitted through the operational unit for OGC review, when time allows.

(U//FOUO) DOJ policy provides that if the AG or his designee authorizes the Director, or his designee to approve an emergency Title III interception, a court order should be sought by filing the affidavit and application, regardless of whether an interception occurs. In the event

that the need for electronic surveillance is eliminated following authorization but prior to the installation and activation of the technical equipment, the submission of an affidavit and application is not necessary.

(U/FOUO) Pursuant to 18 U.S.C. § 2518(7), in the absence of a court order, interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event an application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of Title III, and an inventory shall be served on the person named in the application.

(U/FOUO) The following sample forms are available for use in connection with an emergency Title III request:

- A) (U/FOUO) Emergency Title III Protocol Checklist for CDCs
- B) (U/FOUO) Request for Emergency Title III
- C) (U/FOUO) Emergency Electronic Surveillance Authorization Verification

(U/FOUO) In addition, sample pleadings can be found on the DOJ Net website for the DOJ Electronic Surveillance Unit, or in the DOJ Electronic Surveillance Manual, including:

- A) (U/FOUO) Application for Approval of Emergency Interception of Oral, Wire, or Electronic Communications under 18 U.S.C. § 2518(7)
- B) (U/FOUO) Affidavit in Support of Application for Approval of Emergency Interception of Wire, Oral, or Electronic Communications under 18 U.S.C. § 2518(7)
- C) (U/FOUO) Order Approving Emergency Interception of Wire, Oral, or Electronic Communications under 18 U.S.C. § 2518(7)

18.7.2.8 (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

(U/FOUO) 18 U.S.C. § 2518(1)(c) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. The policy in this DIOG is designed to conform with this statutory requirement, clarify any past confusion, and address the effects on the previous search policy resulting from the recent elimination of the requirement for an agency Action Memorandum by the DOJ OEO. This DIOG policy supersedes the March 5, 2003 Director’s Memorandum to All Special Agents in Charge Re: Pre-Title III Electronic Surveillance (ELSUR) Search Policy, and the April 14, 2008. All Field Offices EC from RMD, Case ID# 321B-HQ-C1186218.

(U) For specific details on how to conduct and document such ELSUR searches, see Appendix H.

18.7.2.9 (U) DURATION OF APPROVAL FOR TITLE III

(U) Court orders issued pursuant to Title III are for a period not to exceed 30 days. An “extension” order may be sought to continue monitoring beyond the initial 30-day period without a lapse in time. When a break in coverage has occurred, a “renewal” order may be sought to continue monitoring the same interceptees and facilities identified in the original order. The affidavit and application in support of an extension or renewal must comply with all of the Title III requirements, including approval of the Attorney General or designee.

18.7.2.10 (U) SPECIFIC PROCEDURES FOR TITLE III AFFIDAVITS

(U//FOUO) The requirements in 18 U.S.C. § 2518 must be followed when preparing a Title III affidavit. The Title III affidavit must include the following information:

- A) (U//FOUO) The identity and qualifications of the affiant must be articulated;
- B) (U//FOUO) For the interception of wire or oral communications, the affidavit must establish probable cause to believe a violation of at least one of the offenses enumerated in 18 U.S.C. § 2516(1) has been, is being, or will be committed. For the interception of electronic communications, the affidavit must establish probable cause to believe that some federal felony has been, is being, or will be committed;
- C) (U//FOUO) The affidavit must set forth the identities of those persons, if known, for whom there is probable cause to believe they are committing the alleged offenses, even if it is not believed they will be intercepted over the target facility. This group of individuals is often referred to as the “Subjects.” “Interceptees” may be listed separately; “interceptee” are those Subjects who are expected to be intercepted;
- D) (U//FOUO) Probable cause must be current and relevant to the use of the particular facilities for which interception is sought;
- E) (U//FOUO) The necessity for the Title III must be articulated. There must be a factual basis for concluding that alternative investigative procedures have been tried and failed or a demonstration why these procedures appear to be unlikely to succeed or would be too dangerous if tried (“boilerplate” statements in this respect are unacceptable);
- F) (U//FOUO) Interceptions must be minimized, as statutorily required;
- G) (U//FOUO) The facility or premises to be intercepted must be described fully, including a diagram, if possible, if microphone installation is contemplated (surreptitious entries may not be conducted for the purpose of preparing a diagram);
- H) (U//FOUO) Whether the request involves any of the seven (7) “sensitive circumstances”; and
- I) (U//FOUO) A statement describing all previous applications for Title III surveillance of the same persons (both subjects and interceptees), facilities or places named in the current affidavit. To comply with this requirement, a “search,” e.g., an automated indices search of the FBI’s ELSUR Records System (ERS) and the systems of other appropriate agencies, must be conducted prior to submitting the Title III affidavit to the DOJ OEO (non-sensitive circumstances) or to the responsible FBIHQ operational unit (sensitive circumstances). The squad SSA is responsible for verifying that pre-Title III ELSUR checks have been completed before the affidavit is sent to the court. The ELSUR Operations Technician (EOT) and the ELSUR supervisor are responsible for confirming that ELSUR searches were properly conducted as set forth in the final affidavit submitted to the court.

(U//FOUO) At least 10 days prior to submitting the original Title III request to DOJ OEO, the field office must forward an electronic communication to FBIHQ setting forth by separate subheading: a synopsis of the investigation; the priority of the investigation within the office; the anticipated manpower and/or linguistic requirements and outside support, if any, that will be needed; a synopsis of the probable cause supporting the Title III application; the prosecutive opinion of the USAO; and description of the interceptees. If a field office is unable to submit the EC 10 days prior to submitting the request to DOJ OEO, the field office must advise the operational unit immediately and note the circumstances that prevent timely notification.

(U//FOUO) Case agents must use the FD-669 (Pre Title III checklist) to guide them through completion of all compliance requirements for Title III.

18.7.2.11 (U) DISPUTE RESOLUTION FOR TITLE III APPLICATIONS

(U//FOUO) When there are legal questions/concerns that cannot be resolved through discussions with reviewing officials at DOJ, the responsible FBIHQ operational division supervisors or executives must forward the application to OGC for its review, advice, and recommendation.

18.7.2.12 (U) NOTICE AND REPORTING REQUIREMENTS – TITLE III

(U//FOUO) The anticipated interception of conversations related to a “Sensitive Investigative Matter” as defined in the AGG-Dom, Part VII.N, requires notice to the appropriate FBIHQ Unit Chief and Section Chief, and DOJ Criminal Division. *Note:* A sensitive investigative matter (SIM) is not the same as a sensitive circumstance described above.

(U//FOUO) Within 14 days of obtaining court authority for an original Title III initiation, the field office must submit a: (i) signed copy of the Title III order and supporting affidavit; (ii) completed CDC Checklist (FD-926); and (iii) FD-669 authorized by the SAC to:

A) (U//FOUO) The appropriate FBIHQ operational unit;

B) (U//FOUO) In applicable drug and money laundering investigations (described in the appropriate CID PG), a copy of the affidavit to Special Operations Division, Chantilly, Virginia;

(U//FOUO) A copy of the DOJ memorandum directed to the AUSA entitled “Authorization for Interception Order Application” must be provided to the EOT.

(U//FOUO) During an authorized intercept, the case agent, in coordination with the prosecuting attorney, must submit periodic investigative activity reports to the authorizing court for oversight of investigative progress (usually every 10 or 15 days). Activity reports must be placed in the investigative file.

(U//FOUO) Within 14 days of the conclusion of Title III ELSUR activity, the case agent must advise the operational FBIHQ investigative program by EC that the surveillance has concluded.

(U//FOUO) Upon completion of Title III ELSUR activity, the Excel WT2 workbook must be submitted by EOU as required by Corporate Policy 0162N. For details on the completion and submission of the Excel WT2 workbook, see Corporate Policy 0162N.

This Page is Intentionally Blank.

**18.7.3 (U) INVESTIGATIVE METHOD: ELECTRONIC SURVEILLANCE – FISA AND FISA
TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)**

18.7.3.1 (U) SUMMARY

(U//FOUO) ELSUR conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) is a valuable investigative method. It is, also, a very intrusive means of acquiring information relevant to the effective execution of the FBI's national security and intelligence missions. To ensure that due consideration is given to the competing interests between national security and the effect on privacy and civil liberties, this section contains various administrative and management controls beyond those imposed by statute and DOJ guidelines. Unless otherwise noted, it is the responsibility of the case agent and his/her supervisor to ensure compliance with these instructions. FISA ELSUR is only authorized as an investigative method in the conduct of Full Investigations. FISA ELSUR requires: (i) administrative or judicial authorization prior to its use; (ii) contact with the field office ELSUR Technician to coordinate all necessary recordkeeping; and (iii) consultation with the Technical Advisor (TA) or a designated TTA to determine feasibility, applicability, and use of the appropriate equipment.

(U//FOUO) **Application:** FISA ELSUR may be used in a Full (national security) Investigation and to collect foreign intelligence information. This method may not be used for: (i) an Assessment or Preliminary Investigation; or (ii) providing assistance to other agencies, unless there is already an FBI FISA related to the request for assistance. Attorney General approval must be obtained prior to using FISA-obtained or derived information in any proceeding whether foreign or domestic. When providing assistance to a foreign agency, information must be provided pursuant to the FBI's Foreign Dissemination Manual and the FBI's Standard Minimization Procedures or other applicable minimization procedures.

(U) This section is divided below into FISA (18.7.3.2) and FISA Title VII (18.7.3.3).

18.7.3.2 (U) FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

18.7.3.2.1 (U) LEGAL AUTHORITY

(U) 50 U.S.C. §§ 1801-1811 (FISA) and E.O. 12333 § 2.5.

(U) FISA Amendments Act of 2008 (P.L.No. 110-261).

18.7.3.2.2 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required.

18.7.3.2.3 (U) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR FISA**18.7.3.2.3.1 (U) FISA REQUEST FORM**

(U//FOUO) FBIHQ and field office requests for FISC ELSUR orders must use the FISA Request Form. Field office requests for FISA orders are submitted and tracked through FISAMS. The FISA request forms, in a question and answer format, have been designed to ensure that all information needed for the preparation of a FISC application is provided to FBIHQ and to the DOJ.

18.7.3.2.3.2 (U) CERTIFICATE BY THE DIRECTOR OF THE FBI

(U) Each FISA application must be accompanied by a Certification by the Director of the FBI or one of nine other individuals authorized by Congress or the President to provide such certifications that: the information being sought is foreign intelligence information; that a significant purpose of the electronic surveillance is to obtain foreign intelligence information; that such information cannot reasonably be obtained by normal investigative techniques; that the information sought is "foreign intelligence information" as defined by FISA. The certification must include a statement explaining the certifier's basis for the certification.

(U) Title 50 of the United States Code Section 1804 specifies the Assistant to the President for National Security Affairs; E.O. 12139 as amended by E.O. 13383 specifies the Director of the FBI, Deputy Director of the FBI, the Director of National Intelligence, the Principal Deputy Director of National Intelligence, the Director of the Central Intelligence Agency, the Secretary of State, the Deputy Secretary of State, the Secretary of Defense, and the Deputy Secretary of Defense as appropriate officials to make certifications required by FISA. The FBI Director has represented to Congress that the FBI Deputy Director will only certify FISA's when the FBI Director is not available to do so.

18.7.3.2.3.3 (U) EMERGENCY FISA AUTHORITY (50 U.S.C. § 1805[F])

(U) The Attorney General, on request from the Director of the FBI or his/her designee, may authorize an emergency FISA for electronic surveillance when it is reasonably determined that an emergency situation exists that precludes advance FISC review and approval and that a factual predication for the issuance of a FISA Order exists. A FISC judge must be informed by DOJ at the time of the emergency authorization and an application must be submitted to that judge as soon as is practicable but not more than seven (7) days after the emergency authority has been approved by the Attorney General. If a court order is denied after an emergency surveillance has been opened, no information gathered as a result of the surveillance may be used as evidence or disclosed in any trial or other proceeding, and no information concerning any USPER acquired from such surveillance may be used or disclosed in any manner, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(U//FOUO) For an emergency FISA for electronic surveillance, DOJ OI can be reached during regular business hours at (202) 514-5600 or through the DOJ Command Center at (202) 514-5000 at any time.

18.7.3.2.4 (U) DURATION OF APPROVAL FOR FISA

(U//FOUO) Authorization for ELSUR surveillance exists for the period of time specified in the FISC's order, which will not exceed: 90 days for USPERs; 120 days for non-USPERs; and one year for a foreign power, as defined in 50 U.S.C. § 1801(a) (1)(2) or (3). For USPERs, renewals of FISA Orders may be requested and authorized for a period of 90 days based upon a continued showing of probable cause. For non-USPERs, renewals can be for a period not to exceed one year. All renewal requests must be submitted to DOJ NSD by the requesting field office at least 45 days prior to the expiration of the existing order. These requests must be submitted using the FISA Request Form process in FISAMS.

18.7.3.2.5 (U//FOUO) SPECIFIC PROCEDURES FOR FISA

(U//FOUO) FISA related initiation and renewal procedures are contained within the FISA Initiation Form which can be found within FISAMS or on the Forms section of the NSLB library.

18.7.3.2.5.1 (U//FOUO) FISA VERIFICATION OF ACCURACY PROCEDURES

(U//FOUO) The accuracy of information contained within FISA applications is of utmost importance; accordingly, the information must be reviewed in accordance with the FISA Accuracy Policy Implementation Guide.

(U//FOUO) Only documented and verified information may be used to support FBI applications to the court. In addition to the certifications required through FISAMS, the following administrative procedures must be followed for every FISA application:

- A) (U//FOUO) Each investigative file for which an application is prepared for submission to the FISC must include a FISA Accuracy sub-file. This sub-file must be used for copies of all of the supporting documentation relied upon when making the certifications contained on the FISA Verification Form ("Woods Form"), which is available in the Forms section of the NSLB library at <http://home.fbinet.fbi/DO/OGC/Main%20Law%20Library/Forms/NSLB%20Library.aspx>

(U//FOUO) The FISA accuracy sub-file must include:

- 1) (U//FOUO) FBI database checks that were conducted to determine whether the target of the proposed FISA is also the subject of an FBI criminal investigation, past or present;
- 2) (U//FOUO) CHS file checks (DELTA, 134, 137, 270, and 307 files) that were conducted to determine whether the target has, or has had, a relationship with the FBI as a CHS; and
- 3) (U//FOUO) Copies of the most authoritative documents that exist for each fact asserted in the application. The most authoritative document may be a cable, EC, letterhead memorandum (LHM), FISA intercept ("tech cut"), etc. The agent must use some judgment in ascertaining appropriate documentation, but, in general, the agent should attempt to get

as close as possible to original documentation of a fact. For example, if the target's immigration status is summarized in an EC, the agent should strive to obtain a copy of the underlying immigration document to verify the fact(s) asserted rather than relying on the EC. Similarly, if the application states that a National Security Letter (NSL) was served on a certain date, there should be a copy of the NSL in the subfile instead of the EC that states an NSL was served. For more guidance on this issue, see FISA Accuracy PG at:

<http://home/forms/fd1028/Policy%20and%20Guidance%20Library/0394PG.pdf>

- B) (U//FOUO) Every FISA application is subject to review through two oversight mechanisms designed to ensure that FBI field offices are taking appropriate steps regarding the factual accuracy of statements to the FISC. First, CDCs in the field are required to conduct accuracy reviews of limited numbers of FISAs in accordance with procedures established by the General Counsel. Second, OI attorneys conduct accuracy reviews with CDC and NSLB participation on approximately an annual basis. A full description of each of these reviews can be found in the FISA Accuracy PG at:

<http://home/forms/fd1028/Policy%20and%20Guidance%20Library/0394PG.pdf>

18.7.3.2.5.2 (U) USE OF FISA DERIVED INFORMATION IN OTHER PROCEEDINGS

(U//FOUO) There are statutory (50 U.S.C. Sections 1806, 1825, and 1845) and Attorney General (AG) policy restrictions on the use of information derived from a FISA ELSUR, physical search, or PR/TT. These restrictions apply to and must be followed by anyone "who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States. . . ." See DIOG Appendix E for the AG Memo, Revised Policy on the Use or Disclosure of FISA Information, dated 01-10-2008. The guidance in the AG's Memo establishes notification/approval procedures which must be strictly followed. Though not contained in the AG Memo, FBI policy requires that use authority be obtained for foreign proceedings as well. Questions concerning the FISA use policy or requests for assistance in obtaining FISA use authority from the AG should be directed to NSLB's Classified Litigation Support Unit.

(U//FOUO) The United States must, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to disclose or use that information or submit it into evidence, notify the "aggrieved person" [as defined in 50 U.S.C. Sections 1801(k), 1821(2), or 1841(2)], and the court or other authority in which the information is to be disclosed or used, that the United States intends to disclose or use such information. See 50 U.S.C. Sections 1806(c), 1825(d), and 1845(c).

18.7.3.2.5.3 (U//FOUO) FISA ELECTRONIC SURVEILLANCE ADMINISTRATIVE SUB-FILE

(U//FOUO) Each investigative file for which an application is or has been prepared for submission to the FISC must include a sub-file labeled FISA Electronic Surveillance Administration Sub-File. This sub-file must contain copies of all applications to and orders issued by the FISC for the conduct of electronic surveillance in the investigation. The following data must be included in the FISA Electronic Surveillance Administrative Sub-file:

A) (U//FOUO) The identities of the persons or entities that are the subject of the electronic surveillance; and

B) (U//FOUO) The description of the facility that is the subject of the electronic surveillance.

18.7.3.2.5.4 (U//FOUO) FISA REVIEW BOARD

(U//FOUO) A FISA Review Board (hereinafter “Board”) has been established that is responsible for reviewing, on a monthly basis, those FISAs (other than certain FISAs from the Counterintelligence Division) that have been maintained for more than one year. The Board’s meeting schedule and requirements for renewal requests are contained and processed through FISAMS.

(U//FOUO) In determining whether to approve continued renewal of a FISA beyond one (1) year, the Board assesses the quality and quantity of foreign intelligence that has been generated by the FISA; the continued need for the foreign intelligence that is being generated by the coverage; the strategy and timing of any criminal prosecution that might be contemplated against the target; any backlog in translation of the results of the surveillance; and the relative risk to national security if the FISA is not renewed.

(U//FOUO) FISAs that are not approved for renewal will be accompanied by an explanation of the reason for denial. FISAs with a dissenting opinion will be forwarded to the EAD NSB for an expeditious review. The Review Board’s decision on renewals with dissenting opinions will be final, unless overruled by the EAD NSB.

18.7.3.2.5.4.1 (U) APPEALING THE DECISION OF THE REVIEW BOARD

(U//FOUO) Should the field office responsible for a FISA disagree with the decision of the Board, the field office responsible for the FISA may present this concern, by EC, to the Assistant Director (AD) responsible for the FISA. The AD will consider the merits of any additional information not previously submitted in writing to the Board and may choose to present a written appeal (EC) for further consideration to the EAD NSB. An EC documenting the decision of the EAD must be provided to the field office promptly upon the EAD’s NSB final decision.

18.7.3.2.6 (U) NOTICE AND REPORTING REQUIREMENTS FOR FISA

(U//FOUO) All FISA related ELSUR notice and reporting requirements can be found in 50 U.S.C §§ 1806-1808 and are contained within FISAMS.

18.7.3.2.7 (U) COMPLIANCE AND MONITORING FOR FISA

(U//FOUO) All compliance issues related to FISA ELSUR must be reported to the Unit Chief of OGC National Security Law Policy and Training Unit, or successor position (soon to be renamed the OGC National Security Law Compliance, Oversight, and Training Unit).

18.7.3.2.8 (U) SPECIAL CIRCUMSTANCES FOR FISA

(U) Under 50 U.S.C. § 1802, the President, through the Attorney General, may authorize electronic surveillance under FISA without a court order for periods of up to one year, if the Attorney General certifies in writing under oath that the surveillance will be solely directed at acquiring communications that are transmitted by means that are exclusively between or among foreign powers and there is no substantial likelihood of the surveillance acquiring the contents of communications to which USPERs are parties.

18.7.3.2.9 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization (“FISA overcollection”) will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

18.7.3.2.10 (U) OTHER APPLICABLE POLICIES**18.7.3.2.10.1 (U) FISA**

- A) (U//FOUO) CD Policy Guide
- B) (U//FOUO) CTD Policy Guide
- C) (U//FOUO) Investigative Law Unit Library
- D) (U//FOUO) Foreign Intelligence Surveillance Act (FISA) Unit

18.7.3.3 (U) FISA TITLE VII (ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION)**18.7.3.3.1 (U) SUMMARY**

(U) Titles I and III of the FISA (codified as 50 U.S.C. §§ 1801, et seq.) provide the standard, traditional methods of collection against agents of foreign powers (including USPERs and non-USPERs) and foreign establishments inside the United States. Title VII of FISA, “Additional Procedures Regarding Certain Persons Outside the United States,” provides the means to target non-USPERs reasonably believed to be located outside the United States.

18.7.3.3.2 (U) LEGAL AUTHORITY

- A) (U) FISA Amendments Act of 2008 (122 Stat 2436)
- B) (U) AGG-Dom, Part V.A.13

18.7.3.3.3 (U) DEFINITION OF INVESTIGATIVE METHOD

(U) Title VII may be used for conducting FISAs on certain persons located outside the United States.

18.7.3.3.4 (U//FOUO) STANDARDS FOR USE AND APPROVAL REQUIREMENTS FOR INVESTIGATIVE METHOD

(U//FOUO) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 and requirements specified above.

18.7.3.3.5 (U) DURATION OF APPROVAL

(U//FOUO) See requirements under DIOG Sections 18.7.1, 18.7.2, and 18.7.3 above.

18.7.3.3.6 (U//FOUO) SPECIFIC COLLECTION PROCEDURES FOR TITLE VII

(U) The relevant procedures (or collections) under Title VII are:

18.7.3.3.6.1 (U) SECTION 702 - PROCEDURES FOR TARGETING NON-U.S. PERSONS (NON-USPERS) WHO ARE OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 702, the Government has the authority to target non-USPERS who are located outside the United States if the collection is effected with the assistance of an electronic communication service provider, as that term is defined in FISA. This section does not require a traditional FISA request. Rather, under this section, the Attorney General and the Director of National Intelligence may authorize, for periods of up to one year, the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information, provided they execute a Certification that is submitted to and approved by the FISC. The Certifications are accompanied by an affidavit signed by the FBI Director. In addition, the FBI is required to file "Targeting Procedures" that ensure that only non-U.S. persons (non-USPERS) reasonably believed to be located outside the United States will be targeted for collection and "to prevent the intentional acquisition of any communications as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." Additionally, the statute prohibits targeting any person reasonably believed to be located outside the United States for the purpose of obtaining the communications of a particular, known person reasonably believed to be in the United States. Finally, the FBI is also required to follow 702-specific minimization procedures.

18.7.3.3.6.2 (U) SECTION 703 - CERTAIN ACQUISITIONS INSIDE THE UNITED STATES TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 703, the Government has the authority to target USPERS who are reasonably believed to be located outside the United States if the collection is effected with the assistance of a United States provider and if the collection occurs inside the United States. This section only authorizes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires a court order, e.g., non-consensual collection. FISA 703 is an alternative to traditional FISA electronic surveillance (Title I) or physical search (Title III) authority when the facts meet the 703 criteria. There are two notable differences between Section 703 and traditional FISA authorities. First, although the application must identify any electronic communication

service provider necessary to effect the acquisition, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 703 allows for the targeting of a USPER who is “an officer or employee of a foreign power,” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order and secondary orders, as needed. The process to obtain that order is the same as the standard FISA process. Refer to the FISA Unit’s website for further information. Section 703 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease immediately if the target enters the United States. If the FBI wishes to continue surveillance of the USPER while he or she is in the United States, the FBI must obtain a separate court order under Title I (electronic surveillance) and/or Title III (physical search) of FISA in order to conduct electronic surveillance or a physical search of that USPER while the person is located in the United States. The use of any information collected using FISA 703 authority must comply with the applicable minimization procedures.

18.7.3.3.6.3 (U) SECTION 704 - OTHER ACQUISITIONS TARGETING UNITED STATES PERSONS OUTSIDE THE UNITED STATES

(U//FOUO) Under Section 704, the Government has the authority to target USPERs who are reasonably believed to be located outside the United States if the collection occurs outside the United States (i.e., without the assistance of a United States’ electronic communication service provider). The statute requires that the FISA court issue an order finding probable cause to believe that the USPER target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power and is reasonably believed to be located outside the United States “under circumstances in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States for law enforcement purposes.” To obtain authority to collect information under this section, the FBI must submit a FISA request and obtain a FISC order (the order will not include secondary orders). The process to obtain a FISA 704 order is similar to, but more streamlined than, that for obtaining a traditional FISA under the standard FISA process. There are two notable differences between Section 704 and traditional FISA authorities. First, the application is not required to identify the specific facilities, places, premises, or property at which the acquisition will be directed. Second, Section 704 allows for the targeting of “an officer or employee of a foreign power” even if the target is not knowingly engaging in clandestine intelligence gathering activities, sabotage, or international terrorism. Refer to the FISA Unit’s intranet website for further information. Section 704 also allows for emergency authorization. Unlike traditional FISA orders, however, surveillance authorized pursuant to this section must cease if the USPER enters the United States but may be re-started if the person is again reasonably believed to be outside the United States during the authorized period of surveillance. If there is a need to continue surveillance while the target is located inside the United States a separate court order must be obtained. The use of any information collected using FISA 704 authority must comply with the applicable minimization procedures.

(U//FOUO) Generally, the FBI requires the assistance of other USIC agencies to implement surveillance authorized pursuant to Section 704. Specific procedures exist for requesting such assistance. These procedures are classified and can be found in FBI Corporate Policy 121N.

18.7.3.3.6.4 (U) SECTION 705 - JOINT APPLICATIONS AND CONCURRENT AUTHORIZATIONS

(U//FOUO) Section 705(a) “joint applications” allow the FISC, upon request of the FBI, to approve a joint application targeting an USPER under both Sections 703 and 704 (authority to collect both when the person is inside and outside the United States).

(U//FOUO) Section 705(b) provides that if an order has been obtained under Section 105 (electronic surveillance under Title I of FISA) or 304 (physical search under Title III of FISA), the Attorney General may authorize the targeting of the USPER target while such person is reasonably believed to be located outside the United States. The Attorney General has this authority under E.O. 12333 § 2.5. In other words, when the FISA Court authorizes surveillance of an USPER target, the Attorney General, under Section 705(b) and E.O. 12333 § 2.5, can simultaneously authorize surveillance to continue if the target travels outside the United States during the authorized period of the surveillance. According to Section 705(b), there is no need for a separate order pursuant to Section 703 or 704. During the FISA drafting process, an FBI employee should determine whether surveillance or physical search may occur for purpose of acquiring foreign intelligence while the person is reasonably believed to be outside the United States. If so, the FBI employee should consult with an OGC or DOJ-NSD attorney to ensure that appropriate language is added to the application.

(U//FOUO) Often when surveilling a USPER overseas, the FBI requires the assistance of other USIC agencies. Specific procedures exist for requesting such assistance. These procedures are classified and can be found in FBI Corporate Policy 121N.

18.7.3.3.6.5 (U) FISA OVERCOLLECTION

(U//FOUO) In accordance with Foreign Intelligence Surveillance Court (FISC) Rule of Procedure 15, information acquired outside of the scope of the FISA authorization (“FISA overcollection”) will no longer be sequestered with the FISC, absent extraordinary circumstances. Contact NSLB for further guidance regarding the handling of any FISA overcollection.

19 (U) ARREST PROCEDURE POLICY

19.1 (U) ARREST WARRANTS

19.1.1 (U) COMPLAINTS

(U) A complaint is a written statement of the facts necessary to establish probable cause to believe that an offense has been committed and that the defendant committed it. A complaint is presented under oath before a magistrate judge, who may issue an arrest warrant or a summons for the defendant if he/she finds the complaint establishes probable cause to believe the defendant committed the charged offense.

19.1.2 (U) ARREST WARRANTS

(U) Any justice, judge or magistrate judge of the United States has the authority to issue arrest warrants for any offense against the United States. In addition, if a federal judge is not available any justice of a state supreme court, mayor of a city, state or local judge, justice of the peace, or other magistrate of any state where the offender may be found can issue such warrants as long as he/she is neutral, detached and capable of deciding probable cause. Copies of warrants issued under this authority are returned to the court of the United States that has jurisdiction over the offense.

19.1.3 (U) JURISDICTION

(U) Federal rules do not limit the application for an arrest warrant to any specified district. Usually, an application for a warrant will be made in the district where the offense was committed, but it may also be issued by a magistrate judge in the district where the offender is located.

19.1.4 (U) PERSON TO BE ARRESTED

(U) An arrest warrant must contain the name of the defendant or, if his/her name is unknown, any name or description by which the defendant can be identified with reasonable certainty. There is no requirement to determine the defendant's true name before a warrant can be issued. It is sufficient to develop facts which provide a reasonable belief that a particular individual is the offender. A warrant can be based on facts that provide a distinguishing physical description or describe the particular circumstances in which the defendant can be found.

19.2 (U) ARREST WITH WARRANT**19.2.1 (U) POLICY**

(U) Whenever possible, an arrest warrant must be obtained prior to an arrest. SSAs may authorize Agents¹⁹ to execute arrest warrants and, in extraordinary circumstances, FBIHQ should be notified in advance of the arrest. For example, SSA's should notify FBIHQ when the arrest may have a significant impact on an investigation in another field office or when the arrest is likely to cause widespread publicity due to the identity or status of the arrestee or the nature of the crime.

(U) Upon the execution of an arrest warrant, the apprehending field office/division must promptly enter a "locate" within NCIC. The OO of the warrant must enter a "clear" within NCIC within 24 hours of the "locate." See the NCIC Field Division Guide, [0145PG](#) for detailed NCIC policy.

19.2.2 (U) PROMPT EXECUTION

(U) While there is no time limit on the execution of arrest warrants (unlike search warrants), as a general rule Agents should make the arrest without prolonged delay after obtaining the warrant.

19.2.3 (U) ARREST PLANS

(U) The SAC is responsible for ensuring that arrests are carefully and thoroughly planned. Proper planning and preparation for arrest situations can greatly enhance the safety and effectiveness of Agents and officers during these high-risk situations. Whenever possible, written arrest plans must be prepared prior to conducting law enforcement activities that may result in the arrest of a potentially dangerous subject. Arrest plans must address five topics: Situation, Mission, Execution, Administration and Equipment, and Control and Communications. The FD-888, FBI Arrest Plan Form, (<http://home.fbinet.fbi/forms/fd1028/SentinelFormsTest/FD888/default.aspx>) must be utilized whenever possible. When briefing the arrest plan, the briefing Agent should stress to the participants of the operation that any arrest has the potential to become dangerous. Exigent circumstances may necessitate an oral briefing in lieu of a written plan, but the oral briefings must address the five topics required to be included in written plans. The planning and execution of arrests, raids, and searches should be assigned to experienced Agents. All arrest plans must be approved by ASACs or their designees.

(U) The SSA may consider utilizing, and/or alerting local authorities to the planned arrest, if appropriate under the circumstances. Although the time of notification is left to the discretion of the SSA, he/she must consider the jurisdiction of local law enforcement, its responsibility to its community and its need to be aware of law enforcement actions in its jurisdiction.

¹⁹ (U) The term "Agent" in the context of this section includes FBI Special Agents and other federal, state, tribal, or local law enforcement officers who have been deputized under either Title 18 or 21 of the United States Code and are working on behalf of or at the direction of the FBI, e.g. task force officer, JTTF, etc.

19.2.4 (U) JOINT ARRESTS

(U) An SSA may authorize a joint arrest with state and local authorities, United States Marshal's Service (USMS), or other federal law enforcement agencies. In circumstances of joint arrests, the SAC remains responsible to ensure that there is a well-considered arrest plan.

19.2.5 (U) POSSESSION AND DISPLAY OF WARRANT

(U) If time permits, the arresting Agent should have the arrest warrant in his/her possession and show it to the defendant at the time of arrest. If the Agent does not have the warrant with him/her at the time of arrest, the Agent must inform the defendant of the offense(s) charged and that a warrant has been issued. The Agent must, at the defendant's request, obtain the warrant and show it to the defendant as soon as practicable.

19.3 (U) ARREST WITHOUT WARRANT

19.3.1 (U) FEDERAL CRIMES

(U) Whenever possible, SAC and USAO authority must be obtained before making a warrantless arrest. Agents are authorized to make warrantless arrests for any federal crime (felony or misdemeanor) committed in their presence. Agents also have authority to make warrantless felony arrests for a crime not committed in the presence of the Agent if there is probable cause to believe the person to be arrested committed a federal felony. A warrantless arrest must only be made when sound judgment indicates obtaining a warrant would unduly burden the investigation or substantially increase the potential for danger or escape. (See Non-Federal Crimes below)

19.3.2 (U) NOTIFICATION TO U.S. ATTORNEY

(U) When a warrantless arrest has been made, the United States Attorney's Office (USAO) must be contacted immediately for authorization to prosecute.

19.3.3 (U) NON-FEDERAL CRIMES

(U) There is no federal statutory authority for Agents to intervene in non-federal (state) crimes. FBI policy permits certain types of non-federal arrests in exigent circumstances.

(U) As a general rule, an Agent should only make an arrest for a state crime if a serious offense (felony or violent misdemeanor) has been committed in his or her presence and immediate action by the Agent is necessary to prevent escape, serious bodily injury, or destruction of property.

(U) Agents are also authorized to arrest a person who is the subject of an FBI Predicated Investigation when a state or local arrest warrant for that person is outstanding, and the person is encountered during the investigation and would likely escape if not arrested. Similarly, an Agent working with state or local law enforcement officers who request assistance to apprehend a nonfederal fugitive who has been encountered during the course of a federal investigation is authorized to provide the requested assistance when intervention is otherwise permitted for a state crime as described in the preceding paragraph.

(U) In some states, there is legislative authority for an Agent to intervene in certain types of state crimes as a peace officer rather than as a private citizen. Deputization as a state peace officer allows a federal Agent to make arrests for state offenses with the authority and immunities of a law enforcement officer of the state or one of its subdivisions. Of greater significance is whether intervention by an Agent in a particular nonfederal crime falls within the scope of employment. Agents who intervene in serious nonfederal crimes committed in their presence or who arrest a state fugitive under the circumstances previously described will normally be considered to be acting within the scope of their employment. While the determination to provide legal representation depends on the facts and circumstances of each circumstance, the DOJ, as a general rule, will provide legal representation to Agents who act in accordance with this policy.

(U) It is important to note that the DOJ has indicated that efforts to enforce minor infractions of the law, such as shoplifting or traffic violations, are not generally considered to be within the scope of employment. Civil actions against federal personnel concerning acts which fall outside the scope of employment will not be removed to federal courts, and employees in such circumstances will not be eligible for legal representation provided for by the DOJ. An Agent's status with respect to civil liability in such circumstances will depend on a particular state's law, which may require an employee to defend himself/herself as an ordinary citizen.

(U) See LHBSA Section 9 for a discussion of potential civil liability when making nonfederal arrests.

19.3.4 (U) ADHERENCE TO FBI POLICY

(U) If any official in the USAO instructs an Agent to arrest or detain a subject in any manner contrary to FBI rules and regulations, the Agent must not comply with such instructions and must immediately inform the SSA. (See the special rules in Section D.13 below for the arrest of juveniles.)

19.4 (U) PROMPT APPEARANCE BEFORE MAGISTRATE

(U) When a federal arrest is made, the arrestee must be taken before the nearest available federal magistrate judge without unnecessary delay. If a federal magistrate judge is not available, the arrestee may be brought before a state or local judicial officer authorized by 18 U.S.C. § 3041 after consultation with the USAO.

(U) Special Considerations for UFAP Arrests: If the arrestee was arrested on a warrant charging only a violation of UFAP, the arrestee can be transferred without unnecessary delay to the custody of the appropriate state or local authorities in the district of arrest. The USAO in the originating district will move promptly to dismiss the UFAP warrant. It is not necessary to wait until the UFAP warrant has been dismissed to release the subject to state or local authorities, but it is important for the Agent to ensure that the USAO dismisses the UFAP warrant promptly after the arrest.

(U) If an Agent makes a warrantless arrest, a complaint must be filed setting forth the probable cause. The complaint is generally submitted when the arrestee is brought before the magistrate. A personal, telephonic, or electronic presentation to the magistrate of the facts setting forth the

probable cause must occur within 48 hours of a warrantless arrest if the arrestee is detained and an initial appearance cannot be held within that 48-hour period.

19.4.1 (U) DEFINITION OF UNNECESSARY DELAY

(U) Rule 5 of the Federal Rules of Criminal Procedure requires the arresting agent to bring the accused before a federal magistrate judge without unnecessary delay. What constitutes “unnecessary delay” is determined in light of all the facts and circumstances. Confessions obtained from defendants during periods of unnecessary delay prior to initial appearance are generally inadmissible at trial. A voluntary confession that occurs within six (6) hours of arrest is admissible if the delay of the initial appearance would be the sole reason for suppression. The six hour period begins when the accused is arrested or taken into custody by federal law enforcement authorities on a federal charge and runs continuously. The six-hour safe harbor can be extended to include delays found by the trial judge to be reasonable considering the means of transportation and the distance to be traveled to the nearest available magistrate judge. Delay for the purpose of conducting interrogation will not be excused. Delays for many other reasons are justified and not grounds for suppression, particularly when there is no indication that the purpose of the delay was to extract a confession. For example, courts have found delays beyond six hours to be justified when attributable to the defendant’s need for medical treatment, his intoxication, the officers’ need to remain at the scene, the unavailability of a magistrate, and booking or other legitimate police procedures unrelated to interrogation.

(U) To avoid the risk that a court will determine that delay beyond the safe-harbor period was “unnecessary” and suppress a confession elicited more than six (6) hours after arrest, Agents who want to continue or resume an interrogation after six (6) hours must seek a waiver of the right to prompt presentment from the accused. To continue an interrogation after six hours have elapsed, Agents must advise the suspect of his Rule 5 rights, and seek an affirmative waiver of those rights from him. The warning and waiver must be substantially in accord with this approved waiver language:

(U) “You have a right to be taken without unnecessary delay to court, where a judge will advise you of the charges against you and provide you with a copy of any affidavit the government has filed in support of these charges. The judge will also advise you of the rights I advised you of previously, namely, that you have a right to an attorney and to have an attorney appointed for you; that you have a right to remain silent and that any statement you make may be used against you. The judge will also tell you that you have a right to a preliminary hearing, at which the government will have to establish that the charges in the complaint are supported by probable cause. The judge will also tell you about the factors that will determine whether you can be released from custody prior to trial. Do you understand this right and are you willing to waive it and continue to talk to us?”

(U) It is prudent to obtain a waiver of the right to prompt presentment in any circumstance when interrogation extends beyond the six-hour safe-harbor period.

19.4.2 (U) EFFECT OF UNNECESSARY DELAY

(U) Incriminating statements obtained during any period of unnecessary delay after arrest and prior to the initial appearance before a magistrate are subject to suppression.

19.4.3 (U) NECESSARY DELAY

(U) If the delay in bringing an arrested person before the magistrate judge is greater than six hours and a confession is obtained *after six hours*, the government has the burden of proving the delay was reasonable. Factors which could contribute to a reasonable delay are the means of transportation, the distance to the nearest available magistrate judge and the time and day of the week of the arrest.

19.4.4 (U) INITIAL PROCESSING

(U) Following an arrest, the defendant should be brought to the nearest FBI office for fingerprinting, photographing, and an interview, where appropriate. Other law enforcement offices may be used for this purpose if FBI facilities are not reasonably available. This process generally should not exceed six hours, measured from the time of arrest to the time of arrival before the magistrate judge.

19.4.5 (U) COLLECTION OF DNA AFTER ARREST OR DETENTION

(U) The Attorney General has directed the FBI to collect DNA samples from all arrestees, other than juveniles, and all non-U.S. persons (non-USPER) lawfully detained. A DNA sample should ordinarily be obtained during initial processing. FBI DNA collection kits should be used to collect a saliva sample from inside the person's mouth.

(U) There is no requirement to obtain a DNA sample from an individual who is arrested on an UFAP warrant when that individual will be turned over to the appropriate state/local agency with the expectation that the UFAP charge will be dismissed. A DNA sample should not be obtained from an individual arrested on a UFAP warrant when there is no expectation of federal prosecution. For example, when it is anticipated that the UFAP charge will be dismissed and the individual turned over to the appropriate state/local agency, no DNA sample should be obtained.

(U) A DNA sample may not be taken from a juvenile arrestee. A DNA sample may only be taken from a juvenile after he/she has been convicted of certain drug or violent offenses.

(U) Federal law requires covered individuals to provide a DNA sample as a condition of pre-trial release and imposes criminal liability for failing to cooperate in the collection of the sample.

(U) The law also authorizes "such means as are reasonably necessary to detain, restrain, and collect a DNA sample from an individual who refuses to cooperate in the collection of the sample." If resistance is encountered, agents must seek to elicit the cooperation of the individual to collect the sample. If the individual continues to resist, agents must advise the USAO or the judge and seek a judicial order requiring the individual to cooperate. If the individual still continues to resist after the court order, agents may use reasonable force to overcome resistance and safely obtain the DNA sample.

(U) For additional information on the process of collecting DNA samples from arrestees, see EC dated, 11/20/2009 from Laboratory to All Field Offices (319T-HQ-A1487667-LAB).

19.5 (U) USE OF FORCE

19.5.1 (U) IDENTIFICATION

(U) An arresting Agent should identify himself/herself before effecting the arrest, in a clear, audible voice, as a Special Agent of the FBI and state his/her intention to arrest the subject.

19.5.2 (U) PHYSICAL FORCE

(U) Agents are permitted to use the amount of physical force reasonable and necessary to take custody and overcome all resistance of the arrestee, and to ensure the safety of the arresting Agents, the arrestee and others in the vicinity of the arrest.

(U) See FBI Deadly Force Policy - DIOG Appendix F.

19.5.3 (U) RESTRAINING DEVICES

(U) Temporary restraining devices, such as handcuffs, shackles and/or belts may be used to secure an arrestee. Use of such devices is lawful and proper, and Agents are expected to employ reasonable judgment under the circumstances in the use of these devices and to resolve any doubt in favor of their use.

19.5.4 (U) PREGNANT ARRESTEES

(U) Within the standard operational procedures designed to ensure the successful completion of an operation and its immediate objectives, and while also guarding the safety of all involved, reasonable precautions and techniques should be employed when dealing with an arrestee reasonably believed to be pregnant to avoid harm to the fetus. This caution includes actions involving confrontation, apprehension, employing restraints, transporting and confining the individual, and respond promptly to needed or requested medical care. In particular, reasonable care or precautions should be considered and used, if appropriate under the circumstances, when employing physical restraints that directly constrict the area of the fetus.

19.6 (U) MANNER OF ENTRY

19.6.1 (U) KNOCK AND ANNOUNCE

(U) Agents are required by law to "knock and announce" their identity, authority and purpose, and demand to enter before entry is made to execute a arrest warrant. This is part of the "reasonableness" requirement of the Fourth Amendment. The announcement can be given by one Agent and need not be lengthy or elaborate but must convey to the person behind the door what is occurring. A loud announcement is essential and electronic devices designed to amplify the voice should be used where communication is anticipated to be difficult. The "knock and announce" requirement need not be complied with when the Agent executing the warrant has a reasonable suspicion of one or more of the following:

- A) (U) to "knock and announce" would cause the Agent and/or another to be placed in imminent peril of bodily harm;

- B) (U) to "knock and announce" would be a useless or futile gesture as the persons within the premises already know of the Agent's identity, authority, and purpose;
- C) (U) to "knock and announce" would cause the evidence sought under the warrant to be destroyed or removed; or
- D) (U) to "knock and announce" would permit the escape of the person the Agent seeks to arrest.

19.6.2 (U) SUSPECT'S PREMISES

(U) In order to lawfully enter a suspect's premises to effect an arrest, Agents must have either: (i) consent to enter, (ii) an emergency ("hot pursuit") justifying a warrantless entry, or (iii) an arrest warrant and probable cause to believe the suspect is in the premises. In determining whether a location is the suspect's premises, an apartment, hotel, motel or boardinghouse room becomes the principal residence of the person renting or leasing such premises. If the suspect is not named on the lease or rental agreement, the premises may still be considered the suspect's premises if the suspect occupies the premises jointly with another.

19.6.3 (U) THIRD PARTY PREMISES

(U) In order to lawfully enter a third party's premises to arrest a suspect, Agents must have either: (i) consent to enter, (ii) an emergency ("hot pursuit") justifying a warrantless entry, or (iii) a search warrant for the third party premises describing the person to be arrested. For these purposes, a "third party premises" is any private premise which is not the principal residence of the person to be arrested. For example, a search warrant would be necessary if the arrestee is an overnight guest, casual visitor, or temporary caller at the premises of the third party. In order to make an entry to arrest, whether premised on an arrest warrant, search warrant, or exigent circumstances, the Agent must have probable cause to believe the suspect to be arrested is within the premises being entered.

19.6.4 (U) EXIGENT CIRCUMSTANCES

(U) If an Agent has a reasonable belief that the subject will flee before a warrant can be obtained, or there is a substantial likelihood that the subject will dispose of evidence before a warrant can be obtained or there is increased danger to Agents or others if entry is delayed to obtain a warrant, exigent circumstances exist which may justify entry into premises to make a warrantless arrest or entry into third party premises without a search warrant to make an arrest.

19.7 (U) SEARCH INCIDENT TO ARREST

(U) The authority to search incident to an arrest is an exception to the warrant requirement. Under this exception, an Agent may conduct a full and complete search of the person of the arrestee and the area within the arrestee's "immediate control." Immediate control means "the area from within which he might gain possession of a weapon or destructible evidence." Once an arrestee has been secured and can no longer reach into the area to be searched, there is no longer justification for a warrantless search. The purpose for the exception is to protect the arresting Agent, prevent escape, and preserve any evidence in possession of the arrestee. The right to search flows from the fact of arrest, not the nature of the crime for which the arrest has been made.

19.7.1 (U) PREREQUISITE: LAWFUL ARREST

(U) For a search incident to arrest to be lawful, the arrest itself must be lawful, i.e. probable cause must exist. Agents can maximize the likelihood that an arrest and search will survive a motion to suppress by obtaining an arrest warrant before effecting the arrest. As discussed below, entry into a subject's premises to arrest may also affect the validity of a search incident to arrest.

(U) Entry into Suspect's Premises: Any entry into premises in order to affect an arrest must be lawful. If entering the defendant's premises to effect the arrest, Agents must have either (i) consent to enter, (ii) an emergency ("hot pursuit"), or (iii) an arrest warrant and probable cause to believe that the defendant is inside the premises.

19.7.2 (U) SCOPE AND TIMING REQUIREMENT

19.7.2.1 (U) SCOPE OF SEARCH

(U) The Agent is entitled to search the person of the arrestee and the area within the arrestee's immediate control at the time of arrest for weapons, to prevent concealment or destruction of evidence, and to prevent concealment of any means of escape. The search may include any portable personal property in the arrestee's actual possession, such as clothing, purses, briefcases, grocery bags, etc. Items of personal property that are accessible to the arrestee, such as an unlocked desk drawer or unlocked suitcase, may be searched. Absent an emergency, inaccessible or locked items of personal property may not be searched. If there is probable cause to believe such items contain evidence, they may be seized, but the Agent must obtain a search warrant prior to opening the item. Once an arrestee has been secured and can no longer reach into the area to be searched, there is no longer justification for a warrantless search.

19.7.2.1.1 (U) VEHICLES

(U) The interior passenger compartment of a vehicle may be searched incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of search or if it is reasonable to believe the vehicle contains evidence of the offense for which the person was arrested. Absent one of these factors, a warrantless search of an arrestee's vehicle is unlawful. For example, a search of the vehicle incident to an arrest would not be permitted after the occupant has been removed, handcuffed, and placed in a nearby Bureau vehicle if the arrest was based on an outstanding arrest warrant for failure to appear. If a search of a vehicle incident to arrest can be done under these factors, the permissible scope can include unlocked or otherwise accessible containers, such as glove compartments, luggage, bags, clothing, etc.

19.7.2.1.2 (U) PROTECTIVE SWEEP

(U) Agents may conduct a protective sweep of the areas immediately adjacent to the site of the arrest for the purpose of locating persons that may pose a threat to the safety of the Agents or others. Additionally, a protective sweep of other areas beyond those immediately adjacent to the site of the arrest may be conducted if the Agents have a reasonable suspicion, based on specific and articulable facts, that an individual who poses a danger to those present is in the

area to be swept. Reasonable suspicion must be based on facts known to the Agents, such as noises in an attic or the at-large status of a dangerous associate. A protective sweep must be limited to a brief inspection of those areas within the premises in which a person could hide. If an Agent observes evidence in plain view while conducting a protective sweep, the evidence may be seized under the plain view doctrine.

19.7.2.2 (U) TIMING

(U) A search incident to arrest must be made contemporaneous to the time and place of arrest and before the arrestee is removed from the area. A further more thorough search of the arrestee at the FBI office or some other place to which the arrestee is transported is also permitted as a search incident to arrest. Additionally, Agents may make protective sweeps as described above at the time of arrest.

19.7.3 (U) INVENTORY OF PERSONAL PROPERTY

(U) Items of personal property removed from a person who has been arrested and is to be incarcerated should be carefully inventoried and promptly, thoroughly searched by Agents prior to being stored for safekeeping. The inventory must include the contents of containers such as purses, shoulder bags, suitcases, etc.

(U) If Agents have probable cause to believe evidence or contraband is in a locked container, a search warrant must be obtained absent emergency circumstances. This is the case because such a search is investigatory in nature. It also falls outside what is permitted as a search incident to arrest because the contents of a locked container are not immediately accessible to the arrestee.

(U) Agents do not need a warrant to conduct an inventory search of a lawfully seized container removed from an arrestee's person. Agents may not, however, conduct an inventory search solely for investigative purposes. The inventory search must strictly adhere to standardized criteria and procedures for collection of property.

19.8 (U) MEDICAL ATTENTION FOR ARRESTEES

(U) If a person in FBI custody complains of sickness or ill health or if it is reasonably apparent to Agents that such a condition exists, arrangements should be made to afford such persons medical attention without delay. Agents must also be mindful of the health and well-being of any pregnant subject and make arrangements for medical attention when asked or when it is reasonably apparent that the subject or fetus needs medical attention. If the time required to obtain medical care may result in the passing of more than six hours between arrest and presentment, Agents must document the basis for and the receipt of any medical attention given to the arrestee.

19.9 (U) ARREST OF FOREIGN NATIONALS

19.9.1 (U) REQUIREMENTS PERTAINING TO FOREIGN NATIONALS

- A) (U) When a foreign national is arrested or detained, the arresting agent must advise him/her of the right to have his/her consular officials notified.

- B) (U) In some situations, the nearest consular officials must be notified of the arrest or detention of a foreign national, regardless of the national's wishes.
- C) (U) Consular officials are entitled to access to their nationals in detention and are entitled to provide consular assistance.

19.9.2 (U) STEPS TO FOLLOW WHEN A FOREIGN NATIONAL IS ARRESTED OR DETAINED

(U) The arresting agent must determine the foreign national's country of citizenship. In the absence of other information, the arresting agent must assume that the country of citizenship is the country on whose passport or other travel documents the foreign national travels.

(U) If the foreign national's country is not on the mandatory notification list below:

- A) (U) The arresting agent must promptly offer to notify the foreign national's consular officials of the arrest/detention. For a suggested statement to the foreign national, see Statement 1 below.
- B) (U) If the foreign national asks that consular notification be given, the arresting Agent must promptly notify the nearest appropriate consular official of the foreign national's arrest.

(U) If the foreign national's country is on the list of mandatory notification countries:

- A) (U) The arresting agent must promptly notify the nearest appropriate consular official of the arrest/detention.
- B) (U) The arresting agent must tell the foreign national that this notification will be made. A suggested statement to the foreign national is found at Statement 2 below.

(U) The arresting agent must keep a written record (EC or FD-302) in the investigative file that he/she provided appropriate notification to the arrestee and of the actions taken.

Mandatory Notification Countries and Jurisdictions

Algeria	Guyana	Saint Lucia
Antigua and Barbuda	Hong Kong ²⁰	Saint Vincent and the Grenadines
Armenia	Hungary	Seychelles
Azerbaijan	Jamaica	Sierra Leone

²⁰ (U) Hong Kong reverted to Chinese sovereignty on July 1, 1997, and is now officially referred to as the Hong Kong Special Administrative Region. Under paragraph 3(f) (2) of the March 25, 1997, U.S.-China Agreement on the Maintenance of the U.S. Consulate General in the Hong Kong Special Administrative Region, U.S. officials are required to notify Chinese officials of the arrest or detention of persons bearing Hong Kong passports in the same manner as is required for persons bearing Chinese passports-- i.e., immediately and, in any event, within four days of the arrest or detention.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

§19

Mandatory Notification Countries and Jurisdictions

Bahamas	Kazakhstan	Singapore
Barbados	Kiribati	Slovakia
Belarus	Kuwait	Tajikistan
Belize	Kyrgyzstan	Tanzania
Brunei	Malaysia	Tonga
Bulgaria	Malta	Trinidad and Tobago
China ²¹	Mauritius	Tunisia
Costa Rica	Moldova	Turkmenistan
Cyprus	Mongolia	Tuvalu
Czech Republic	Nigeria	Ukraine
Dominica	Philippines	United Kingdom ²²
Fiji	Poland (non-permanent residents only)	U.S.S.R.
Gambia	Romania	Uzbekistan
Georgia	Russia	Zambia
Ghana	Saint Kitts and Nevis	Zimbabwe
Grenada		

²¹ (U) Notification is not mandatory in the case of persons who carry "Republic of China" passports issued by Taiwan. Such persons must be informed without delay, that the nearest office of the Taipei Economic and Cultural Representative Office ("TECRO"), the unofficial entity representing Taiwan's interests in the United States, can be notified at their request.

²² (U) Mandatory notification is required for nationals of the British dependencies Anguilla, British Virgin Islands, Bermuda, Montserrat, and the Turks and Caicos Islands. Their nationals carry United Kingdom passports.

19.9.3 (U) SUGGESTED STATEMENTS TO ARRESTED OR DETAINED FOREIGN NATIONALS

19.9.3.1 (U) STATEMENT 1: WHEN CONSULAR NOTIFICATION IS AT THE FOREIGN NATIONAL'S OPTION

(U) You are entitled to have us notify your country's consular representatives here in the United States that you have been arrested or detained. A consular official from your country may be able to help you obtain legal counsel and may contact your family and visit you in detention, among other things. If you want us to notify your country's consular officials, you can request notification now or at any time in the future. After your consular officials are notified, they may call or visit you. Do you want us to notify your country's consular officials?

19.9.3.2 (U) STATEMENT 2: WHEN CONSULAR NOTIFICATION IS MANDATORY

(U) Because of your nationality, we are required to notify your country's consular representatives here in the United States that you have been arrested or detained. After your consular officials are notified, they may call or visit you. You are not required to accept their assistance, but they may be able to help you obtain legal counsel and may contact your family and visit you in detention, among other things. We will notify your country's consular officials as soon as possible.

19.9.4 (U) DIPLOMATIC IMMUNITY

(U) Diplomatic representatives of foreign governments in the United States may not be arrested. Agents may not enter the office or dwelling of a diplomat or a person with diplomatic immunity for the purpose of making an arrest, search, or seizure.

19.9.4.1 (U) TERRITORIAL IMMUNITY

(U) All embassies, legations, and consulates have territorial immunity. Consequently, no Agent may attempt to enter any embassy, legation, or consulate for the purpose of making an arrest, search or seizure. This territorial immunity extends to both the offices and residences of ambassadors and ministers, but only to the office of a consul. A consul's residence does not enjoy territorial immunity.

19.9.4.2 (U) PERSONAL IMMUNITY

(U) Ambassadors and ministers, members of their staffs and domestic servants, and the immediate family members of a diplomatic officer have personal immunity, as do the immediate family members of the administrative and technical staff of a diplomatic mission. Consequently, no Agent should attempt to arrest or detain any such person. The personal immunity applies to the staffs, domestic servants and immediate family members, regardless of citizenship. Ordinarily, consuls do not have personal immunity from arrest on misdemeanor charges. If the arrest of a consul is contemplated, immediately notify FBIHQ by telephone or electronic communication before any action is taken so that an appropriate check

can be made with the Department of State to determine whether the consul involved has any special immunity.

19.10 (U) ARREST OF NEWS MEDIA MEMBERS

(U) Attorney General approval must be obtained prior to seeking an arrest warrant for or arresting a member of the news media who is suspected of committing any federal offense in the course of, or arising out of, the coverage or investigation of a news story, or while engaged in the performance of official news media duties.

(U) Requests for the approval must be submitted to the AD of the operational FBIHQ division that is responsible for the investigative classification and the AD of the Office of Public Affairs (OPA) by an EC. The requesting EC must be reviewed by the CDC and approved by the SAC after coordination with the local USAO. The EC must set forth the facts believed to establish probable cause and the investigative justification for the arrest, consistent with the DOJ guidelines set forth in 28 C.F.R. § 50.10.

(U) In emergency circumstances, an Agent may arrest a member of the news media without prior AG approval, if authorized by the SAC and the USAO. In such situations, the SAC must immediately notify the AD of the FBIHQ operational division, the AD of the OPA, and the General Counsel of the arrest, the emergency circumstances that justified proceeding without prior authorization and all of the information that would have been provided if prior authorization had been sought. The AD of the operational division must promptly notify the appropriate officials at DOJ as established in 28 C.F.R. § 50.10. After these oral notifications have been made, the field office must provide written documentation to the FBIHQ operational AD as soon as practicable, but not more than 24 hours after the arrest. FBIHQ must provide appropriate written documentation to the DOJ approval authorities to whom oral notice was given.

19.11 (U) ARREST OF ARMED FORCES PERSONNEL

(U) The Uniform Code of Military Justice authorizes any commanding officer exercising general court-martial jurisdiction to surrender military personnel under the officer's command to civil authority when the person has been charged with a civil offense. A request for surrender must be accompanied by:

- A) (U) A copy of the indictment, presentment, information, or warrant;
- B) (U) Sufficient information to identify the person sought as the person who allegedly committed the offense; and
- C) (U) A statement of the maximum sentence which may be imposed upon conviction.

(U) Receipts for persons surrendered for civil prosecution should be signed by an official in the USAO, not by an FBI employee.

19.12 (U) ARREST OF JUVENILES

19.12.1 (U) DEFINITION

(U) A violation of 18 U.S.C. § 922(x)(2) or violation a federal law which would have been a crime, if committed by an adult, by a person who has not attained his/her 18th birthday is an act of juvenile delinquency. For the purpose of juvenile delinquency proceedings, a juvenile is a person who committed a crime before his/her 18th birthday who has not attained his/her 21st birthday at the time charges are commenced.

19.12.2 (U) ARREST PROCEDURES

(U) Prearrest procedures applicable to adults (discussion with USAO, filing of complaint, issuance of warrant) also govern arrests of juveniles. After arrest, however, the Federal Juvenile Delinquency Act requires strict compliance with the following procedures:

- A) (U) **Advice of Rights** - The arresting Agent must immediately advise the arrested juvenile of his/her "legal rights" in language comprehensible to the juvenile. The rights found on the standard Form FD-395 meet this requirement. The arresting Agent may obtain a signature waiving his/her rights only if the Chief Division Counsel (CDC) or the USAO, based on the law of the circuit, has approved interrogation of the juvenile.
- B) (U) **Notification to U.S. Attorney's Office and Juvenile's Parents** - The arresting Agent must immediately notify the USAO and the juvenile's parents, guardian, or custodian, that the juvenile has been arrested. The juvenile's parents, guardian, or custodian must also be notified of the juvenile's rights (use the FD-395 for this purpose) and the nature of the alleged offense for which the juvenile was arrested.
- C) (U) **Initial Appearance before Magistrate Judge** - Subsequent to his/her arrest, the juvenile must be taken to a magistrate judge forthwith.
- D) (U) **Record of Notification and Appearance** - Because proof of timely notification to the juvenile's parents and prompt appearance before the magistrate judge is essential, Agents must promptly prepare FD-302(s) documenting the time the following events occurred:
 - 1) (U) The juvenile was arrested;
 - 2) (U) The juvenile was advised of his/her rights;
 - 3) (U) The USAO was notified;
 - 4) (U) The juvenile's parents, guardian, or custodian were notified of the arrest and of the juvenile's rights; and
 - 5) (U) The juvenile was taken before a magistrate judge.
- E) (U) **Interrogation and Interviews** - Whether a juvenile may be interrogated between arrest for a federal offense and initial appearance before the magistrate judge depends on the law of the circuit in which the arrest occurs. If interrogation is not permitted in the circuit of arrest, information volunteered by the arrested juvenile concerning his/her guilt must be recorded in the Agent's FD-302. Clarifying questions may be asked if necessary to be certain what the juvenile intended to convey. The volunteered statement may be reduced to writing if such action does not delay the juvenile's appearance before the magistrate judge. A juvenile may always be questioned concerning the guilt of someone else, if such questioning does not delay bringing him/her before the magistrate judge. These rules apply only when the juvenile has

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

been arrested for a federal offense. They do not apply when the juvenile is suspected of having committed a federal offense but is under arrest by state or local officers on a state or local charge.

- F) (U) **Fingerprinting and Photographing** - Agents may not fingerprint or photograph a juvenile unless he/she is to be prosecuted as an adult. Because it is not known at the time of arrest whether the juvenile will be prosecuted as an adult or a juvenile, Agents may not fingerprint or photograph a juvenile without permission of the magistrate judge. Following an adjudication of delinquency based on an offense which, if committed by an adult, would be a felony that is a crime of violence or a violation of 21 U.S.C. § 841 (manufacturing, distributing, dispensing of a controlled substance or possession with the intent to do same), § 955 (possession of controlled substances on board vessels arriving in or departing the United States) or § 959 (manufacture or distribution of controlled substances for purpose of unlawful importation), the juvenile must be fingerprinted and photographed. Agents should coordinate fingerprinting and photographing with the USMS.
- G) (U) **DNA Collection** - Agents must not take DNA samples from juveniles at the time of arrest.
- H) (U) **Press Releases** - Neither the name nor picture of an arrested juvenile may be made public. Accordingly, the arrest of a juvenile may only be announced by a press release that does not contain identifying information.

20 (U) OTHER INVESTIGATIVE RESOURCES

20.1 (U) OVERVIEW

(U) Other investigative resources described below are available as specified in Assessments and Predicated Investigations. The investigative resources include:

20.1.1 (U//FOUO) NAME TRACE REQUESTS (CIA AND NSA)

(U) See Section 20.2 below.

20.1.2 (U//FOUO) BLIND FAITH PROGRAM

(U) See Section 20.3 below.

20.1.3 (U//FOUO) BEHAVIORAL ANALYSIS – OPERATIONAL BEHAVIORAL SUPPORT PROGRAM

(U) See Section 20.4 below.

20.1.4 (U//FOUO) SENSITIVE TECHNICAL EQUIPMENT

(U) See Section 20.5 below.

20.2 (U//FOUO) NAME TRACE REQUESTS (CIA AND NSA)

(U//FOUO) A Name Trace Request is a formal request to another government agency to conduct a search of its existing records for information regarding a subject of interest.

20.2.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U//FOUO) CIA and NSA Name Trace Requests may be used in Assessments and Predicated Investigations.

(U) See the classified provisions in DIOG Appendix G for additional information on making a Name Trace Request.

20.3 (U//FOUO) BLIND FAITH PROGRAM

(U//FOUO) The Blind Faith Program is an analytical program which provides a technical countermeasures profile for targets of investigative interest to the FBI. These profiles assess the technical sophistication of the intelligence service of a particular target in order to determine its capability to detect and/or nullify technical attacks directed against it. Awareness of a target's capabilities prior to a technical installation permits the selection of technologies appropriate to the level of sophistication of that target, thereby conserving resources. The program reports the

results of its analysis in the form of a Blind Faith report, which details and describes the technical sophistication of the target.

20.3.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U//FOUO) The Blind Faith Program may be used in Assessments and Predicated Investigations.

(U//FOUO) The Blind Faith Program is operated by the Operational Technology Division, Technical Operations Coordination Unit, Technical Evaluation Office (TEO).

20.4 (U//FOUO) OPERATIONAL BEHAVIORAL SUPPORT PROGRAM – CIRG’S BEHAVIORAL ANALYSIS UNITS (BAUs) AND/OR CD’S BEHAVIORAL ANALYSIS PROGRAM

20.4.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U) The National Center for the Analysis of Violent Crime (NCAVC) manages and directs the FBI’s operational behavioral support across all investigative programs. In addition, the NCAVC’s units provide operational and analytical support, without charge, to federal, state, local, tribal, foreign law enforcement, intelligence and security agencies involved in the investigation of unusual or repetitive violent crimes, communicated threats, terrorism, and other matters. The NCAVC also provides support through expertise and consultation in non-violent matters, such as national security, corruption, and white-collar crime investigations. See DIOG Section 12 for FD-999 documentation and other requirements for Assistance to Other Agencies.

(U) Requests for NCAVC operational assistance should be made to the NCAVC Coordinator in the field office or to the NCAVC unit at Quantico. Requests for service can be coordinated through direct contact, telephone, email or Electronic Communication to the NCAVC. All FBI operational behavioral support requests must be coordinated and approved by the NCAVC.

(U) The appropriate Legal Attaché office (Legat) or the International Operations Division (IOD) must coordinate all requests from foreign law enforcement, intelligence and security agencies with NCAVC staff. NCAVC staff will assist the Legat or IOD preparation of an appropriate request for service and will facilitate the delivery of the service requested from the foreign agency.

(U) For additional information regarding the services provided by NCAVC.

20.5 (U//FOUO) SENSITIVE TECHNICAL EQUIPMENT

(U//FOUO) Definition: Sensitive Technical Equipment (STE) is defined in the classified provisions in DIOG Appendix G.

20.5.1 (U) AUTHORIZED INVESTIGATIVE ACTIVITY

(U) The use of STE for electronic or physical surveillance may be authorized in Predicated Investigations as set forth in OTD policy. See the classified provisions in DIOG Appendix G for additional information.

(U//FOUO) All use of STE outside the United States requires the prior approval of the HQ operational division responsible for the investigation, the IOD, and the Operational Technology Division (OTD). Refer to the Extraterritorial Guidelines (see DIOG Section 13), appropriate Policy Implementation Guides, and OTD policy for additional information.

This Page is Intentionally Blank.

21 (U) INTELLIGENCE COLLECTION

21.1 (U) INCIDENTAL COLLECTION

(U//FOUO) Intelligence that is responsive to PFI requirements, FBI national collection requirements, and FBI field office collection requirements may be collected incidental to an Assessment or Predicated Investigation. When information that is responsive to these requirements is incidentally collected in an Assessment or Predicated Investigation, it should be forwarded to the Field Intelligence Group (FIG) for evaluation and potential dissemination against collection requirements. (See DIOG Section 15.6.1.2 - Written Intelligence Products) All incidental collection must be documented in the 8151 field office file.

(U//FOUO) Prior to submitting to the FIG any information that may be evidentiary and therefore potentially discoverable, the FBI employee should discuss with the CDC or OGC the potential impact disseminating the information in an intelligence product may have on the prosecution of the investigation. To the extent dissemination might or is likely to have an adverse impact on the prosecution, the FBI, in consultation with the prosecuting attorney, must assess whether the need for dissemination outweighs the probable impact the dissemination may have on the prosecution.

21.2 (U) FBI NATIONAL COLLECTION REQUIREMENTS

(U//FOUO) The FBIHQ DI establishes FBI national collection requirements after coordination with OGC, other FBIHQ operational divisions, and field offices. An FBI national collection requirement describes information needed by the FBI to: (i) identify or obtain information about potential targets of, or vulnerabilities to, Federal criminal activities or threats to the national security; or (ii) inform or facilitate intelligence analysis and planning pertinent to the FBI's law enforcement or national security missions.

(U//FOUO) FBI intelligence needs may correspond with "Foreign Intelligence Requirements" issued under the authority of the DNI. An FBI national collection requirement should not be confused with a PFI requirement. A PFI requirement addresses the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons that are not directly related to the FBI's core national security and law enforcement missions.

(U) For example:

- A) (U//FOUO) The USIC seeks information on the presence of Tamil Tigers inside the United States. FBIHQ DI accepts this requirement because it corresponds to the national security mission of the FBI and a National Collection Requirement is published to the full FBI. The field office could open a Type 3 Assessment in the appropriate national security classification to determine the existence and extent of the threat posed to the United States by the Tamil Tigers in its AOR. Any information collected during this Type 3 Assessment can be used to answer this National Collection Requirement and be disseminated appropriately to the USIC.
- B) (U//FOUO) The USIC seeks information regarding the intentions of the Republic of X to strengthen its military in the wake of hostile actions by the Government of Y. If FBIHQ DI accepts this requirement as a PFI requirement, a file in the 809-814, or 816 investigative classification series will be opened by the DI. A field office could open a Type 6 Assessment

to determine if it has the capacity to respond to this requirement in the 809-814, or 816 series file.

- C) (U//FOUO) The USIC seeks information regarding the Government of Y's intentions vis-à-vis the Republic of X. FBIHQ DI accepts this requirement as a PFI Collection Requirement and opens a file in the 809-814, or 816 investigative classification series. As part of an existing counterintelligence Predicated Investigation, an investigative squad has technical coverage that is yielding information pertinent to this PFI Collection requirement. The investigative squad should share all of the foreign intelligence collected during the course of its investigation with the FIG, which will analyze and disseminate that foreign intelligence information and document its handling of the intelligence in the appropriate 809-814, or 816 classification file.

(U//FOUO) Before any investigative activity is conducted in order to respond to an FBI national collection requirement, an Assessment or Predicated Investigation must be opened or already open. An Assessment cannot be opened solely based upon an FBI national collection requirement. An authorized purpose (national security or criminal threat) and clearly defined objective(s) must exist prior to opening an Assessment. During an Assessment, the FBI is authorized to collect against any FBI national collection requirement that is relevant to the Assessment. The FBI is authorized to open an Assessment (or a Full Investigation) to collect on a USIC intelligence requirement only if it has been accepted and designated by FBIHQ DI as a PFI Collection Requirement, as specified in DIOG Section 9.

(U//FOUO) To ensure continuity in the dissemination of reporting against collection requirements, FBIHQ DI provides a unique requirement citation number for each FBI national collection and PFI requirement. The FBIHQ DI will determine the method for capturing and tracking these referenced unique identifiers.

(U//FOUO) FBIHQ DI provides specific guidance in its policy implementation guide regarding FBI national collection requirements, FBI field office collection requirements (see Section 21.3, below) and PFI requirements.

21.3 (U//FOUO) FBI FIELD OFFICE COLLECTION REQUIREMENTS

(U//FOUO) An FBI field office collection requirement describes information needed by the field to: (i) identify or obtain information about potential targets of or vulnerabilities to Federal criminal activities or threats to the national security; or (ii) inform or facilitate intelligence analysis and planning pertinent to the FBI's law enforcement or national security missions.

(U//FOUO) Before any investigative activity may be conducted to respond to an FBI field office collection requirement, an Assessment or Predicated Investigation must be opened or already open. An Assessment cannot be opened solely based upon an FBI field office collection requirement. Following coordination with the CDC, FBI field office collection requirements are established by the Intelligence Program Coordinator (SSA or SIA), consistent with FBI National Priorities as established by FBIHQ. FBI field office collection requirements may only be levied against the field office creating the requirement. All FBI field office collection requirements must receive a unique requirement citation in accordance with the classified FBI Corporate Requirements Policy. The IPG contains detailed guidance regarding the field office collection requirements.

APPENDIX A: (U) THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS

PREAMBLE

These Guidelines are issued under the authority of the Attorney General as provided in sections 509, 510, 533, and 534 of title 28, United States Code, and Executive Order 12333. They apply to domestic investigative activities of the Federal Bureau of Investigation (FBI) and other activities as provided herein.

TABLE OF CONTENTS

INTRODUCTION	5
A. FBI RESPONSIBILITIES – FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE	6
B. THE FBI AS AN INTELLIGENCE AGENCY	9
C. OVERSIGHT	10
I. <u>GENERAL AUTHORITIES AND PRINCIPLES</u>	12
A. SCOPE	12
B. GENERAL AUTHORITIES	12
C. USE OF AUTHORITIES AND METHODS	12
D. NATURE AND APPLICATION OF THE GUIDELINES	14
II. <u>INVESTIGATIONS AND INTELLIGENCE GATHERING</u>	16
A. ASSESSMENTS	19
B. PREDICATED INVESTIGATIONS	20
C. ENTERPRISE INVESTIGATIONS	23
III. <u>ASSISTANCE TO OTHER AGENCIES</u>	25
A. THE INTELLIGENCE COMMUNITY	25
B. FEDERAL AGENCIES GENERALLY	25
C. STATE, LOCAL, OR TRIBAL AGENCIES	27
D. FOREIGN AGENCIES	27
E. APPLICABLE STANDARDS AND PROCEDURES	28
IV. <u>INTELLIGENCE ANALYSIS AND PLANNING</u>	29
A. STRATEGIC INTELLIGENCE ANALYSIS	29
B. REPORTS AND ASSESSMENTS GENERALLY	29
C. INTELLIGENCE SYSTEMS	29
V. <u>AUTHORIZED METHODS</u>	31
A. PARTICULAR METHODS	31
B. SPECIAL REQUIREMENTS	32
C. OTHERWISE ILLEGAL ACTIVITY	33
VI. <u>RETENTION AND SHARING OF INFORMATION</u>	35
A. RETENTION OF INFORMATION	35
B. INFORMATION SHARING GENERALLY	35
C. INFORMATION RELATING TO CRIMINAL MATTERS	36
D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS	37

VII. DEFINITIONS 42

INTRODUCTION

As the primary investigative agency of the federal government, the Federal Bureau of Investigation (FBI) has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role in carrying out investigations within the United States of threats to the national security. This includes the lead domestic role in investigating international terrorist threats to the United States, and in conducting counterintelligence activities to meet foreign entities' espionage and intelligence efforts directed against the United States. The FBI is also vested with important functions in collecting foreign intelligence as a member agency of the U.S. Intelligence Community. The FBI accordingly plays crucial roles in the enforcement of federal law and the proper administration of justice in the United States, in the protection of the national security, and in obtaining information needed by the United States for the conduct of its foreign affairs. These roles reflect the wide range of the FBI's current responsibilities and obligations, which require the FBI to be both an agency that effectively detects, investigates, and prevents crimes, and an agency that effectively protects the national security and collects intelligence.

The general objective of these Guidelines is the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States. At the same time, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people. The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

The issuance of these Guidelines represents the culmination of the historical evolution of the FBI and the policies governing its domestic operations subsequent to the September 11, 2001, terrorist attacks on the United States. Reflecting decisions and directives of the President and the Attorney General, inquiries and enactments of Congress, and the conclusions of national commissions, it was recognized that the FBI's functions needed to be expanded and better integrated to meet contemporary realities:

[C]ontinuing coordination . . . is necessary to optimize the FBI's performance in both national security and criminal investigations [The] new reality requires first that the FBI and other agencies do a better job of gathering intelligence inside the United States, and second that we eliminate the remnants of the old "wall" between foreign intelligence and domestic law enforcement. Both tasks must be accomplished without sacrificing our domestic liberties and the rule of law, and both depend on building a very

different FBI from the one we had on September 10, 2001. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 466, 452 (2005).)

In line with these objectives, the FBI has reorganized and reoriented its programs and missions, and the guidelines issued by the Attorney General for FBI operations have been extensively revised over the past several years. Nevertheless, the principal directives of the Attorney General governing the FBI's conduct of criminal investigations, national security investigations, and foreign intelligence collection have persisted as separate documents involving different standards and procedures for comparable activities. These Guidelines effect a more complete integration and harmonization of standards, thereby providing the FBI and other affected Justice Department components with clearer, more consistent, and more accessible guidance for their activities, and making available to the public in a single document the basic body of rules for the FBI's domestic operations.

These Guidelines also incorporate effective oversight measures involving many Department of Justice and FBI components, which have been adopted to ensure that all FBI activities are conducted in a manner consistent with law and policy.

The broad operational areas addressed by these Guidelines are the FBI's conduct of investigative and intelligence gathering activities, including cooperation and coordination with other components and agencies in such activities, and the intelligence analysis and planning functions of the FBI.

A. FBI RESPONSIBILITIES – FEDERAL CRIMES, THREATS TO THE NATIONAL SECURITY, FOREIGN INTELLIGENCE

Part II of these Guidelines authorizes the FBI to carry out investigations to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. The major subject areas of information gathering activities under these Guidelines – federal crimes, threats to the national security, and foreign intelligence – are not distinct, but rather overlap extensively. For example, an investigation relating to international terrorism will invariably crosscut these areas because international terrorism is included under these Guidelines' definition of "threat to the national security," because international terrorism subject to investigation within the United States usually involves criminal acts that violate federal law, and because information relating to international terrorism also falls within the definition of "foreign intelligence." Likewise, counterintelligence activities relating to espionage are likely to concern matters that constitute threats to the national security, that implicate violations or potential violations of federal espionage laws, and that involve information falling under the definition of "foreign intelligence."

While some distinctions in the requirements and procedures for investigations are necessary in different subject areas, the general design of these Guidelines is to take a uniform

approach wherever possible, thereby promoting certainty and consistency regarding the applicable standards and facilitating compliance with those standards. Hence, these Guidelines do not require that the FBI's information gathering activities be differentially labeled as "criminal investigations," "national security investigations," or "foreign intelligence collections," or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI's legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security and to further the United States' foreign intelligence objectives. In many cases, a single investigation will be supportable as an exercise of a number of these authorities – i.e., as an investigation of a federal crime or crimes, as an investigation of a threat to the national security, and/or as a collection of foreign intelligence.

1. Federal Crimes

The FBI has the authority to investigate all federal crimes that are not exclusively assigned to other agencies. In most ordinary criminal investigations, the immediate objectives include such matters as: determining whether a federal crime has occurred or is occurring, or if planning or preparation for such a crime is taking place; identifying, locating, and apprehending the perpetrators; and obtaining the evidence needed for prosecution. Hence, close cooperation and coordination with federal prosecutors in the United States Attorneys' Offices and the Justice Department litigating divisions are essential both to ensure that agents have the investigative tools and legal advice at their disposal for which prosecutorial assistance or approval is needed, and to ensure that investigations are conducted in a manner that will lead to successful prosecution. Provisions in many parts of these Guidelines establish procedures and requirements for such coordination.

2. Threats to the National Security

The FBI's authority to investigate threats to the national security derives from the executive order concerning U.S. intelligence activities, from delegations of functions by the Attorney General, and from various statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq. These Guidelines (Part VII.S) specifically define threats to the national security to mean: international terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or any successor order.

Activities within the definition of "threat to the national security" that are subject to investigation under these Guidelines commonly involve violations (or potential violations) of federal criminal laws. Hence, investigations of such threats may constitute an exercise both of the FBI's criminal investigation authority and of the FBI's authority to investigate threats to the national security. As with criminal investigations generally, detecting and solving the crimes, and eventually arresting and prosecuting the perpetrators, are likely to be among the objectives of

investigations relating to threats to the national security. But these investigations also often serve important purposes outside the ambit of normal criminal investigation and prosecution, by providing the basis for, and informing decisions concerning, other measures needed to protect the national security. These measures may include, for example: excluding or removing persons involved in terrorism or espionage from the United States; recruitment of double agents; freezing assets of organizations that engage in or support terrorism; securing targets of terrorism or espionage; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism or other national security threats.

In line with this broad range of purposes, investigations of threats to the national security present special needs to coordinate with other Justice Department components, including particularly the Justice Department's National Security Division, and to share information and cooperate with other agencies with national security responsibilities, including other agencies of the U.S. Intelligence Community, the Department of Homeland Security, and relevant White House (including National Security Council and Homeland Security Council) agencies and entities. Various provisions in these Guidelines establish procedures and requirements to facilitate such coordination.

3. Foreign Intelligence

As with the investigation of threats to the national security, the FBI's authority to collect foreign intelligence derives from a mixture of administrative and statutory sources. See, e.g., E.O. 12333; 50 U.S.C. 401 et seq.; 50 U.S.C. 1801 et seq.; 28 U.S.C. 532 note (incorporating P.L. 108-458 §§ 2001-2003). These Guidelines (Part VII.E) define foreign intelligence to mean "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists."

The FBI's foreign intelligence collection activities have been expanded by legislative and administrative reforms subsequent to the September 11, 2001, terrorist attacks, reflecting the FBI's role as the primary collector of foreign intelligence within the United States, and the recognized imperative that the United States' foreign intelligence collection activities become more flexible, more proactive, and more efficient in order to protect the homeland and adequately inform the United States' crucial decisions in its dealings with the rest of the world:

The collection of information is the foundation of everything that the Intelligence Community does. While successful collection cannot ensure a good analytical product, the failure to collect information . . . turns analysis into guesswork. And as our review demonstrates, the Intelligence Community's human and technical intelligence collection agencies have collected far too little information on many of the issues we care about most. (Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 351 (2005).)

These Guidelines accordingly provide standards and procedures for the FBI's foreign intelligence collection activities that meet current needs and realities and optimize the FBI's ability to discharge its foreign intelligence collection functions.

The authority to collect foreign intelligence extends the sphere of the FBI's information gathering activities beyond federal crimes and threats to the national security, and permits the FBI to seek information regarding a broader range of matters relating to foreign powers, organizations, or persons that may be of interest to the conduct of the United States' foreign affairs. The FBI's role is central to the effective collection of foreign intelligence within the United States because the authorized domestic activities of other intelligence agencies are more constrained than those of the FBI under applicable statutes and Executive Order 12333. In collecting foreign intelligence, the FBI will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives issued under the authority of the Director of National Intelligence (DNI). As provided in Part VII.F of these Guidelines, foreign intelligence requirements may also be established by the President or Intelligence Community officials designated by the President, and by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

The general guidance of the FBI's foreign intelligence collection activities by DNI-authorized requirements does not, however, limit the FBI's authority to conduct investigations supportable on the basis of its other authorities – to investigate federal crimes and threats to the national security – in areas in which the information sought also falls under the definition of foreign intelligence. The FBI conducts investigations of federal crimes and threats to the national security based on priorities and strategic objectives set by the Department of Justice and the FBI, independent of DNI-established foreign intelligence collection requirements.

Since the authority to collect foreign intelligence enables the FBI to obtain information pertinent to the United States' conduct of its foreign affairs, even if that information is not related to criminal activity or threats to the national security, the information so gathered may concern lawful activities. The FBI should accordingly operate openly and consensually with U.S. persons to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

B. THE FBI AS AN INTELLIGENCE AGENCY

The FBI is an intelligence agency as well as a law enforcement agency. Its basic functions accordingly extend beyond limited investigations of discrete matters, and include broader analytic and planning functions. The FBI's responsibilities in this area derive from various administrative and statutory sources. See, e.g., E.O. 12333; 28 U.S.C. 532 note (incorporating P.L. 108-458 §§ 2001-2003) and 534 note (incorporating P.L. 109-162 § 1107). Enhancement of the FBI's intelligence analysis capabilities and functions has consistently been recognized as a key priority in the legislative and administrative reform efforts following the

September 11, 2001, terrorist attacks:

[Counterterrorism] strategy should . . . encompass specific efforts to . . . enhance the depth and quality of domestic intelligence collection and analysis . . . [T]he FBI should strengthen and improve its domestic [intelligence] capability as fully and expeditiously as possible by immediately instituting measures to . . . significantly improve strategic analytical capabilities (Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, S. Rep. No. 351 & H.R. Rep. No. 792, 107th Cong., 2d Sess. 4-7 (2002) (errata print).)

A “smart” government would *integrate* all sources of information to see the enemy as a whole. Integrated all-source analysis should also inform and shape strategies to collect more intelligence. . . . The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to “connect the dots.” (Final Report of the National Commission on Terrorist Attacks Upon the United States 401, 408 (2004).)

Part IV of these Guidelines accordingly authorizes the FBI to engage in intelligence analysis and planning, drawing on all lawful sources of information. The functions authorized under that Part include: (i) development of overviews and analyses concerning threats to and vulnerabilities of the United States and its interests, (ii) research and analysis to produce reports and assessments concerning matters relevant to investigative activities or other authorized FBI activities, and (iii) the operation of intelligence systems that facilitate and support investigations through the compilation and analysis of data and information on an ongoing basis.

C. OVERSIGHT

The activities authorized by these Guidelines must be conducted in a manner consistent with all applicable laws, regulations, and policies, including those protecting privacy and civil liberties. The Justice Department’s National Security Division and the FBI’s Inspection Division, Office of General Counsel, and Office of Integrity and Compliance, along with other components, share the responsibility to ensure that the Department meets these goals with respect to national security and foreign intelligence matters. In particular, the National Security Division’s Oversight Section, in conjunction with the FBI’s Office of General Counsel, is responsible for conducting regular reviews of all aspects of FBI national security and foreign intelligence activities. These reviews, conducted at FBI field offices and headquarter units, broadly examine such activities for compliance with these Guidelines and other applicable requirements.

Various features of these Guidelines facilitate the National Security Division’s oversight functions. Relevant requirements and provisions include: (i) required notification by the FBI to the National Security Division concerning full investigations that involve foreign intelligence collection or investigation of United States persons in relation to threats of the national security, (ii) annual reports by the FBI to the National Security Division concerning the FBI’s foreign

intelligence collection program, including information on the scope and nature of foreign intelligence collection activities in each FBI field office, and (iii) access by the National Security Division to information obtained by the FBI through national security or foreign intelligence activities and general authority for the Assistant Attorney General for National Security to obtain reports from the FBI concerning these activities.

Pursuant to these Guidelines, other Attorney General guidelines, and institutional assignments of responsibility within the Justice Department, additional Department components – including the Criminal Division, the United States Attorneys’ Offices, and the Office of Privacy and Civil Liberties – are involved in the common endeavor with the FBI of ensuring that the activities of all Department components are lawful, appropriate, and ethical as well as effective. Examples include the involvement of both FBI and prosecutorial personnel in the review of undercover operations involving sensitive circumstances, notice requirements for investigations involving sensitive investigative matters (as defined in Part VII.N of these Guidelines), and notice and oversight provisions for enterprise investigations, which may involve a broad examination of groups implicated in the gravest criminal and national security threats. These requirements and procedures help to ensure that the rule of law is respected in the Department’s activities and that public confidence is maintained in these activities.

I. GENERAL AUTHORITIES AND PRINCIPLES

A. SCOPE

These Guidelines apply to investigative activities conducted by the FBI within the United States or outside the territories of all countries. They do not apply to investigative activities of the FBI in foreign countries, which are governed by the Attorney General's Guidelines for Extraterritorial FBI Operations.

B. GENERAL AUTHORITIES

1. The FBI is authorized to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in Part II of these Guidelines.
2. The FBI is authorized to provide investigative assistance to other federal agencies, state, local, or tribal agencies, and foreign agencies as provided in Part III of these Guidelines.
3. The FBI is authorized to conduct intelligence analysis and planning as provided in Part IV of these Guidelines.
4. The FBI is authorized to retain and share information obtained pursuant to these Guidelines as provided in Part VI of these Guidelines.

C. USE OF AUTHORITIES AND METHODS

1. Protection of the United States and Its People

The FBI shall fully utilize the authorities provided and the methods authorized by these Guidelines to protect the United States and its people from crimes in violation of federal law and threats to the national security, and to further the foreign intelligence objectives of the United States.

2. Choice of Methods

- a. The conduct of investigations and other activities authorized by these Guidelines may present choices between the use of different investigative methods that are each operationally sound and effective, but that are more or less intrusive, considering such factors as the effect on the privacy and civil liberties of individuals and potential damage to reputation. The least intrusive method feasible is to be used in such situations. It is recognized,

however, that the choice of methods is a matter of judgment. The FBI shall not hesitate to use any lawful method consistent with these Guidelines, even if intrusive, where the degree of intrusiveness is warranted in light of the seriousness of a criminal or national security threat or the strength of the information indicating its existence, or in light of the importance of foreign intelligence sought to the United States' interests. This point is to be particularly observed in investigations relating to terrorism.

- b. United States persons shall be dealt with openly and consensually to the extent practicable when collecting foreign intelligence that does not concern criminal activities or threats to the national security.

3. Respect for Legal Rights

All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States. These Guidelines also do not authorize any conduct prohibited by the Guidance Regarding the Use of Race by Federal Law Enforcement Agencies.

4. Undisclosed Participation in Organizations

Undisclosed participation in organizations in activities under these Guidelines shall be conducted in accordance with FBI policy approved by the Attorney General.

5. Maintenance of Records under the Privacy Act

The Privacy Act restricts the maintenance of records relating to certain activities of individuals who are United States persons, with exceptions for circumstances in which the collection of such information is pertinent to and within the scope of an authorized law enforcement activity or is otherwise authorized by statute. 5 U.S.C. 552a(e)(7). Activities authorized by these Guidelines are authorized law enforcement activities or activities for which there is otherwise statutory authority for purposes of the Privacy Act. These Guidelines, however, do not provide an exhaustive enumeration of authorized FBI law enforcement activities or FBI activities for which there is otherwise statutory authority, and no restriction is implied with respect to such activities carried out by the FBI pursuant to other

authorities. Further questions about the application of the Privacy Act to authorized activities of the FBI should be addressed to the FBI Office of the General Counsel, the FBI Privacy and Civil Liberties Unit, or the Department of Justice Office of Privacy and Civil Liberties.

D. NATURE AND APPLICATION OF THE GUIDELINES

1. Repealers

These Guidelines supersede the following guidelines, which are hereby repealed:

- a. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (May 30, 2002) and all predecessor guidelines thereto.
- b. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (October 31, 2003) and all predecessor guidelines thereto.
- c. The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence (November 29, 2006).
- d. The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations (August 8, 1988).
- e. The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest (April 5, 1976).

2. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice.

3. Departures from the Guidelines

Departures from these Guidelines must be approved by the Director of the FBI, by the Deputy Director of the FBI, or by an Executive Assistant Director designated

by the Director. If a departure is necessary without such prior approval because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director, the Deputy Director, or a designated Executive Assistant Director shall be notified as soon thereafter as practicable. The FBI shall provide timely written notice of departures from these Guidelines to the Criminal Division and the National Security Division, and those divisions shall notify the Attorney General and the Deputy Attorney General. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

4. Other Activities Not Limited

These Guidelines apply to FBI activities as provided herein and do not limit other authorized activities of the FBI, such as the FBI's responsibilities to conduct background checks and inquiries concerning applicants and employees under federal personnel security programs, the FBI's maintenance and operation of national criminal records systems and preparation of national crime statistics, and the forensic assistance and administration functions of the FBI Laboratory.

II. INVESTIGATIONS AND INTELLIGENCE GATHERING

This Part of the Guidelines authorizes the FBI to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence.

When an authorized purpose exists, the focus of activities authorized by this Part may be whatever the circumstances warrant. The subject of such an activity may be, for example, a particular crime or threatened crime; conduct constituting a threat to the national security; an individual, group, or organization that may be involved in criminal or national security-threatening conduct; or a topical matter of foreign intelligence interest.

Investigations may also be undertaken for protective purposes in relation to individuals, groups, or other entities that may be targeted for criminal victimization or acquisition, or for terrorist attack or other depredations by the enemies of the United States. For example, the participation of the FBI in special events management, in relation to public events or other activities whose character may make them attractive targets for terrorist attack, is an authorized exercise of the authorities conveyed by these Guidelines. Likewise, FBI counterintelligence activities directed to identifying and securing facilities, personnel, or information that may be targeted for infiltration, recruitment, or acquisition by foreign intelligence services are authorized exercises of the authorities conveyed by these Guidelines.

The identification and recruitment of human sources – who may be able to provide or obtain information relating to criminal activities, information relating to terrorism, espionage, or other threats to the national security, or information relating to matters of foreign intelligence interest – is also critical to the effectiveness of the FBI's law enforcement, national security, and intelligence programs, and activities undertaken for this purpose are authorized and encouraged.

The scope of authorized activities under this Part is not limited to "investigation" in a narrow sense, such as solving particular cases or obtaining evidence for use in particular criminal prosecutions. Rather, these activities also provide critical information needed for broader analytic and intelligence purposes to facilitate the solution and prevention of crime, protect the national security, and further foreign intelligence objectives. These purposes include use of the information in intelligence analysis and planning under Part IV, and dissemination of the information to other law enforcement, Intelligence Community, and White House agencies under Part VI. Information obtained at all stages of investigative activity is accordingly to be retained and disseminated for these purposes as provided in these Guidelines, or in FBI policy consistent with these Guidelines, regardless of whether it furthers investigative objectives in a narrower or more immediate sense.

In the course of activities under these Guidelines, the FBI may incidentally obtain information relating to matters outside of its areas of primary investigative responsibility. For example, information relating to violations of state or local law or foreign law may be

incidentally obtained in the course of investigating federal crimes or threats to the national security or in collecting foreign intelligence. These Guidelines do not bar the acquisition of such information in the course of authorized investigative activities, the retention of such information, or its dissemination as appropriate to the responsible authorities in other agencies or jurisdictions. Part VI of these Guidelines includes specific authorizations and requirements for sharing such information with relevant agencies and officials.

This Part authorizes different levels of information gathering activity, which afford the FBI flexibility, under appropriate standards and procedures, to adapt the methods utilized and the information sought to the nature of the matter under investigation and the character of the information supporting the need for investigation.

Assessments, authorized by Subpart A of this Part, require an authorized purpose but not any particular factual predication. For example, to carry out its central mission of preventing the commission of terrorist acts against the United States and its people, the FBI must proactively draw on available sources of information to identify terrorist threats and activities. It cannot be content to wait for leads to come in through the actions of others, but rather must be vigilant in detecting terrorist activities to the full extent permitted by law, with an eye towards early intervention and prevention of acts of terrorism before they occur. Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage. The proactive investigative authority conveyed in assessments is designed for, and may be utilized by, the FBI in the discharge of these responsibilities. For example, assessments may be conducted as part of the FBI's special events management activities.

More broadly, detecting and interrupting criminal activities at their early stages, and preventing crimes from occurring in the first place, is preferable to allowing criminal plots and activities to come to fruition. Hence, assessments may be undertaken proactively with such objectives as detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization by such activities; and identifying and assessing individuals who may have value as human sources. For example, assessment activities may involve proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place; through which child pornography is advertised and traded; through which efforts are made by sexual predators to lure children for purposes of sexual abuse; or through which fraudulent schemes are perpetrated against the public.

The methods authorized in assessments are generally those of relatively low intrusiveness, such as obtaining publicly available information, checking government records,

and requesting information from members of the public. These Guidelines do not impose supervisory approval requirements in assessments, given the types of techniques that are authorized at this stage (e.g., perusing the Internet for publicly available information). However, FBI policy will prescribe supervisory approval requirements for certain assessments, considering such matters as the purpose of the assessment and the methods being utilized.

Beyond the proactive information gathering functions described above, assessments may be used when allegations or other information concerning crimes or threats to the national security is received or obtained, and the matter can be checked out or resolved through the relatively non-intrusive methods authorized in assessments. The checking of investigative leads in this manner can avoid the need to proceed to more formal levels of investigative activity, if the results of an assessment indicate that further investigation is not warranted.

Subpart B of this Part authorizes a second level of investigative activity, predicated investigations. The purposes or objectives of predicated investigations are essentially the same as those of assessments, but predication as provided in these Guidelines is needed – generally, allegations, reports, facts or circumstances indicative of possible criminal or national security-threatening activity, or the potential for acquiring information responsive to foreign intelligence requirements – and supervisory approval must be obtained, to initiate predicated investigations. Corresponding to the stronger predication and approval requirements, all lawful methods may be used in predicated investigations. A classified directive provides further specification concerning circumstances supporting certain predicated investigations.

Predicated investigations that concern federal crimes or threats to the national security are subdivided into preliminary investigations and full investigations. Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal or national security-threatening activity, but more substantial factual predication is required for full investigations. While time limits are set for the completion of preliminary investigations, full investigations may be pursued without preset limits on their duration.

The final investigative category under this Part of the Guidelines is enterprise investigations, authorized by Subpart C, which permit a general examination of the structure, scope, and nature of certain groups and organizations. Enterprise investigations are a type of full investigations. Hence, they are subject to the purpose, approval, and predication requirements that apply to full investigations, and all lawful methods may be used in carrying them out. The distinctive characteristic of enterprise investigations is that they concern groups or organizations that may be involved in the most serious criminal or national security threats to the public – generally, patterns of racketeering activity, terrorism or other threats to the national security, or the commission of offenses characteristically involved in terrorism as described in 18 U.S.C. 2332b(g)(5)(B). A broad examination of the characteristics of groups satisfying these criteria is authorized in enterprise investigations, including any relationship of the group to a foreign power, its size and composition, its geographic dimensions and finances, its past acts and goals, and its capacity for harm.

A. ASSESSMENTS

1. Purposes

Assessments may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval

The conduct of assessments is subject to any supervisory approval requirements prescribed by FBI policy.

3. Authorized Activities

Activities that may be carried out for the purposes described in paragraph 1. in an assessment include:

- a. seeking information, proactively or in response to investigative leads, relating to:
 - i. activities constituting violations of federal criminal law or threats to the national security,
 - ii. the involvement or role of individuals, groups, or organizations in such activities; or
 - iii. matters of foreign intelligence interest responsive to foreign intelligence requirements;
- b. identifying and obtaining information about potential targets of or vulnerabilities to criminal activities in violation of federal law or threats to the national security;
- c. seeking information to identify potential human sources, assess the suitability, credibility, or value of individuals as human sources, validate human sources, or maintain the cover or credibility of human sources, who may be able to provide or obtain information relating to criminal activities in violation of federal law, threats to the national security, or matters of foreign intelligence interest; and
- d. obtaining information to inform or facilitate intelligence analysis and planning as described in Part IV of these Guidelines.

4. Authorized Methods

Only the following methods may be used in assessments:

- a. Obtain publicly available information.
- b. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
- c. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
- d. Use online services and resources (whether nonprofit or commercial).
- e. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
- f. Interview or request information from members of the public and private entities.
- g. Accept information voluntarily provided by governmental or private entities.
- h. Engage in observation or surveillance not requiring a court order.
- i. Grand jury subpoenas for telephone or electronic mail subscriber information.

B. PREDICATED INVESTIGATIONS

1. Purposes

Predicated investigations may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence.

2. Approval

The initiation of a predicated investigation requires supervisory approval at a level or levels specified by FBI policy. A predicated investigation based on paragraph 3.c. (relating to foreign intelligence) must be approved by a Special Agent in Charge or by an FBI Headquarters official as provided in such policy.

3. Circumstances Warranting Investigation

A predicated investigation may be initiated on the basis of any of the following circumstances:

- a. An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity.
- b. An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the investigation may obtain information that would help to protect against such activity or threat.
- c. The investigation may obtain foreign intelligence that is responsive to a foreign intelligence requirement.

4. Preliminary and Full Investigations

A predicated investigation relating to a federal crime or threat to the national security may be conducted as a preliminary investigation or a full investigation. A predicated investigation that is based solely on the authority to collect foreign intelligence may be conducted only as a full investigation.

a. Preliminary investigations

i. Predication Required for Preliminary Investigations

A preliminary investigation may be initiated on the basis of information or an allegation indicating the existence of a circumstance described in paragraph 3.a.-b.

ii. Duration of Preliminary Investigations

A preliminary investigation must be concluded within six months of its initiation, which may be extended by up to six months by the Special Agent in Charge. Extensions of preliminary investigations beyond a year must be approved by FBI Headquarters.

iii. Methods Allowed in Preliminary Investigations

All lawful methods may be used in a preliminary investigation except for methods within the scope of Part V.A.11.-.13. of these Guidelines.

b. Full Investigations

i. Predication Required for Full Investigations

A full investigation may be initiated if there is an articulable factual basis for the investigation that reasonably indicates that a circumstance described in paragraph 3.a.-b. exists or if a circumstance described in paragraph 3.c. exists.

ii. Methods Allowed in Full Investigations

All lawful methods may be used in a full investigation.

5. Notice Requirements

- a. An FBI field office shall notify FBI Headquarters and the United States Attorney or other appropriate Department of Justice official of the initiation by the field office of a predicated investigation involving a sensitive investigative matter. If the investigation is initiated by FBI Headquarters, FBI Headquarters shall notify the United States Attorney or other appropriate Department of Justice official of the initiation of such an investigation. If the investigation concerns a threat to the national security, an official of the National Security Division must be notified. The notice shall identify all sensitive investigative matters involved in the investigation.
- b. The FBI shall notify the National Security Division of:
 - i. the initiation of any full investigation of a United States person relating to a threat to the national security; and
 - ii. the initiation of any full investigation that is based on paragraph 3.c. (relating to foreign intelligence).
- c. The notifications under subparagraphs a. and b. shall be made as soon as practicable, but no later than 30 days after the initiation of an investigation.

- d. The FBI shall notify the Deputy Attorney General if FBI Headquarters disapproves a field office's initiation of a predicated investigation relating to a threat to the national security on the ground that the predication for the investigation is insufficient.

C. ENTERPRISE INVESTIGATIONS

1. Definition

A full investigation of a group or organization may be initiated as an enterprise investigation if there is an articulable factual basis for the investigation that reasonably indicates that the group or organization may have engaged or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

- a. a pattern of racketeering activity as defined in 18 U.S.C. 1961(5);
- b. international terrorism or other threat to the national security;
- c. domestic terrorism as defined in 18 U.S.C. 2331(5) involving a violation of federal criminal law;
- d. furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
- e. an offense described in 18 U.S.C. 2332b(g)(5)(B) or 18 U.S.C. 43.

2. Scope

The information sought in an enterprise investigation may include a general examination of the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; and its past and future activities and goals.

3. Notice and Reporting Requirements

- a. The responsible Department of Justice component for the purpose of notification and reports in enterprise investigations is the National Security Division, except that, for the purpose of notifications and reports in an enterprise investigation relating to a pattern of racketeering activity that does not involve an offense or offenses described in 18 U.S.C. 2332b(g)(5)(B), the responsible Department of Justice component is the

Organized Crime and Racketeering Section of the Criminal Division.

- b. An FBI field office shall notify FBI Headquarters of the initiation by the field office of an enterprise investigation.
- c. The FBI shall notify the National Security Division or the Organized Crime and Racketeering Section of the initiation of an enterprise investigation, whether by a field office or by FBI Headquarters, and the component so notified shall notify the Attorney General and the Deputy Attorney General. The FBI shall also notify any relevant United States Attorney's Office, except that any investigation within the scope of Part VI.D.1.d of these Guidelines (relating to counterintelligence investigations) is to be treated as provided in that provision. Notifications by the FBI under this subparagraph shall be provided as soon as practicable, but no later than 30 days after the initiation of the investigation.
- d. The Assistant Attorney General for National Security or the Chief of the Organized Crime and Racketeering Section, as appropriate, may at any time request the FBI to provide a report on the status of an enterprise investigation and the FBI will provide such reports as requested.

III. ASSISTANCE TO OTHER AGENCIES

The FBI is authorized to provide investigative assistance to other federal, state, local, or tribal, or foreign agencies as provided in this Part.

The investigative assistance authorized by this Part is often concerned with the same objectives as those identified in Part II of these Guidelines – investigating federal crimes and threats to the national security, and collecting foreign intelligence. In some cases, however, investigative assistance to other agencies is legally authorized for purposes other than those identified in Part II, such as assistance in certain contexts to state or local agencies in the investigation of crimes under state or local law, see 28 U.S.C. 540, 540A, 540B, and assistance to foreign agencies in the investigation of foreign law violations pursuant to international agreements. Investigative assistance for such legally authorized purposes is permitted under this Part, even if it is not for purposes identified as grounds for investigation under Part II.

The authorities provided by this Part are cumulative to Part II and do not limit the FBI's investigative activities under Part II. For example, Subpart B.2 in this Part authorizes investigative activities by the FBI in certain circumstances to inform decisions by the President concerning the deployment of troops to deal with civil disorders, and Subpart B.3 authorizes investigative activities to facilitate demonstrations and related public health and safety measures. The requirements and limitations in these provisions for conducting investigations for the specified purposes do not limit the FBI's authority under Part II to investigate federal crimes or threats to the national security that occur in the context of or in connection with civil disorders or demonstrations.

A. THE INTELLIGENCE COMMUNITY

The FBI may provide investigative assistance (including operational support) to authorized intelligence activities of other Intelligence Community agencies.

B. FEDERAL AGENCIES GENERALLY

1. In General

The FBI may provide assistance to any federal agency in the investigation of federal crimes or threats to the national security or in the collection of foreign intelligence, and investigative assistance to any federal agency for any other purpose that may be legally authorized, including investigative assistance to the Secret Service in support of its protective responsibilities.

2. The President in Relation to Civil Disorders

- a. At the direction of the Attorney General, the Deputy Attorney General, or

the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to actual or threatened civil disorders to assist the President in determining (pursuant to the authority of the President under 10 U.S.C. 331-33) whether use of the armed forces or militia is required and how a decision to commit troops should be implemented. The information sought shall concern such matters as:

- i. The size of the actual or threatened disorder, both in number of people involved or affected and in geographic area.
 - ii. The potential for violence.
 - iii. The potential for expansion of the disorder in light of community conditions and underlying causes of the disorder.
 - iv. The relationship of the actual or threatened disorder to the enforcement of federal law or court orders and the likelihood that state or local authorities will assist in enforcing those laws or orders.
 - v. The extent of state or local resources available to handle the disorder.
- b. Investigations under this paragraph will be authorized only for a period of 30 days, but the authorization may be renewed for subsequent 30 day periods.
 - c. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

3. Public Health and Safety Authorities in Relation to Demonstrations

- a. At the direction of the Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division, the FBI shall collect information relating to demonstration activities that are likely to require the federal government to take action to facilitate the activities and provide public health and safety measures with respect to those activities. The information sought in such an investigation shall be that needed to facilitate an adequate federal response to ensure public health and safety

and to protect the exercise of First Amendment rights, such as:

- i. The time, place, and type of activities planned.
 - ii. The number of persons expected to participate.
 - iii. The expected means and routes of travel for participants and expected time of arrival.
 - iv. Any plans for lodging or housing of participants in connection with the demonstration.
- b. Notwithstanding Subpart E.2 of this Part, the methods that may be used in an investigation under this paragraph are those described in subparagraphs a.-d., subparagraph f. (other than pretext interviews or requests), or subparagraph g. of Part II.A.4 of these Guidelines. The Attorney General, the Deputy Attorney General, or the Assistant Attorney General for the Criminal Division may also authorize the use of other methods described in Part II.A.4.

C. STATE, LOCAL, OR TRIBAL AGENCIES

The FBI may provide investigative assistance to state, local, or tribal agencies in the investigation of matters that may involve federal crimes or threats to the national security, or for such other purposes as may be legally authorized.

D. FOREIGN AGENCIES

1. At the request of foreign law enforcement, intelligence, or security agencies, the FBI may conduct investigations or provide assistance to investigations by such agencies, consistent with the interests of the United States (including national security interests) and with due consideration of the effect on any United States person. Investigations or assistance under this paragraph must be approved as provided by FBI policy. The FBI shall notify the National Security Division concerning investigation or assistance under this paragraph where: (i) FBI Headquarters approval for the activity is required pursuant to the approval policy adopted by the FBI for purposes of this paragraph, and (ii) the activity relates to a threat to the national security. Notification to the National Security Division shall be made as soon as practicable but no later than 30 days after the approval. Provisions regarding notification to or coordination with the Central Intelligence Agency by the FBI in memoranda of understanding or agreements with the Central Intelligence Agency may also apply to activities under this paragraph.
2. The FBI may not provide assistance to foreign law enforcement, intelligence, or

security officers conducting investigations within the United States unless such officers have provided prior notification to the Attorney General as required by 18 U.S.C. 951.

3. The FBI may conduct background inquiries concerning consenting individuals when requested by foreign government agencies.
4. The FBI may provide other material and technical assistance to foreign governments to the extent not otherwise prohibited by law.

E. APPLICABLE STANDARDS AND PROCEDURES

1. Authorized investigative assistance by the FBI to other agencies under this Part includes joint operations and activities with such agencies.
2. All lawful methods may be used in investigative assistance activities under this Part.
3. Where the methods used in investigative assistance activities under this Part go beyond the methods authorized in assessments under Part II.A.4 of these Guidelines, the following apply:
 - a. Supervisory approval must be obtained for the activity at a level or levels specified in FBI policy.
 - b. Notice must be provided concerning sensitive investigative matters in the manner described in Part II.B.5.
 - c. A database or records system must be maintained that permits, with respect to each such activity, the prompt retrieval of the status of the activity (open or closed), the dates of opening and closing, and the basis for the activity. This database or records system may be combined with the database or records system for predicated investigations required by Part VI.A.2.

IV. INTELLIGENCE ANALYSIS AND PLANNING

The FBI is authorized to engage in analysis and planning. The FBI's analytic activities enable the FBI to identify and understand trends, causes, and potential indicia of criminal activity and other threats to the United States that would not be apparent from the investigation of discrete matters alone. By means of intelligence analysis and strategic planning, the FBI can more effectively discover crimes, threats to the national security, and other matters of national intelligence interest and can provide the critical support needed for the effective discharge of its investigative responsibilities and other authorized activities. For example, analysis of threats in the context of special events management, concerning public events or activities that may be targeted for terrorist attack, is an authorized activity under this Part.

In carrying out its intelligence functions under this Part, the FBI is authorized to draw on all lawful sources of information, including but not limited to the results of investigative activities under these Guidelines. Investigative activities under these Guidelines and other legally authorized activities through which the FBI acquires information, data, or intelligence may properly be utilized, structured, and prioritized so as to support and effectuate the FBI's intelligence mission. The remainder of this Part provides further specification concerning activities and functions authorized as part of that mission.

A. STRATEGIC INTELLIGENCE ANALYSIS

The FBI is authorized to develop overviews and analyses of threats to and vulnerabilities of the United States and its interests in areas related to the FBI's responsibilities, including domestic and international criminal threats and activities; domestic and international activities, circumstances, and developments affecting the national security; and matters relevant to the conduct of the United States' foreign affairs. The overviews and analyses prepared under this Subpart may encompass present, emergent, and potential threats and vulnerabilities, their contexts and causes, and identification and analysis of means of responding to them.

B. REPORTS AND ASSESSMENTS GENERALLY

The FBI is authorized to conduct research, analyze information, and prepare reports and assessments concerning matters relevant to authorized FBI activities, such as reports and assessments concerning: types of criminals or criminal activities; organized crime groups; terrorism, espionage, or other threats to the national security; foreign intelligence matters; or the scope and nature of criminal activity in particular geographic areas or sectors of the economy.

C. INTELLIGENCE SYSTEMS

The FBI is authorized to operate intelligence, identification, tracking, and information

systems in support of authorized investigative activities, or for such other or additional purposes as may be legally authorized, such as intelligence and tracking systems relating to terrorists, gangs, or organized crime groups.

V. AUTHORIZED METHODS

A. PARTICULAR METHODS

All lawful investigative methods may be used in activities under these Guidelines as authorized by these Guidelines. Authorized methods include, but are not limited to, those identified in the following list. The methods identified in the list are in some instances subject to special restrictions or review or approval requirements as noted:

1. The methods described in Part II.A.4 of these Guidelines.
2. Mail covers.
3. Physical searches of personal or real property where a warrant or court order is not legally required because there is no reasonable expectation of privacy (e.g., trash covers).
4. Consensual monitoring of communications, including consensual computer monitoring, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. Where a sensitive monitoring circumstance is involved, the monitoring must be approved by the Criminal Division or, if the investigation concerns a threat to the national security or foreign intelligence, by the National Security Division.
5. Use of closed-circuit television, direction finders, and other monitoring devices, subject to legal review by the Chief Division Counsel or the FBI Office of the General Counsel. (The methods described in this paragraph usually do not require court orders or warrants unless they involve physical trespass or non-consensual monitoring of communications, but legal review is necessary to ensure compliance with all applicable legal requirements.)
6. Polygraph examinations.
7. Undercover operations. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover operations must be carried out in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. In investigations that are not subject to the preceding sentence because they concern threats to the national security or foreign intelligence, undercover operations involving religious or political organizations must be reviewed and approved by FBI Headquarters, with participation by the National Security Division in the review process.
8. Compulsory process as authorized by law, including grand jury subpoenas and

other subpoenas, National Security Letters (15 U.S.C. 1681u, 1681v; 18 U.S.C. 2709; 12 U.S.C. 3414(a)(5)(A); 50 U.S.C. 436), and Foreign Intelligence Surveillance Act orders for the production of tangible things (50 U.S.C. 1861-63).

9. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of title 18, United States Code (18 U.S.C. 2701-2712).
10. Use of pen registers and trap and trace devices in conformity with chapter 206 of title 18, United States Code (18 U.S.C. 3121-3127), or the Foreign Intelligence Surveillance Act (50 U.S.C. 1841-1846).
11. Electronic surveillance in conformity with chapter 119 of title 18, United States Code (18 U.S.C. 2510-2522), the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5.
12. Physical searches, including mail openings, in conformity with Rule 41 of the Federal Rules of Criminal Procedure, the Foreign Intelligence Surveillance Act, or Executive Order 12333 § 2.5. A classified directive provides additional limitation on certain searches.
13. Acquisition of foreign intelligence information in conformity with title VII of the Foreign Intelligence Surveillance Act.

B. SPECIAL REQUIREMENTS

Beyond the limitations noted in the list above relating to particular investigative methods, the following requirements are to be observed:

1. Contacts with Represented Persons

Contact with represented persons may implicate legal restrictions and affect the admissibility of resulting evidence. Hence, if an individual is known to be represented by counsel in a particular matter, the FBI will follow applicable law and Department procedure concerning contact with represented individuals in the absence of prior notice to counsel. The Special Agent in Charge and the United States Attorney or their designees shall consult periodically on applicable law and Department procedure. Where issues arise concerning the consistency of contacts with represented persons with applicable attorney conduct rules, the United States Attorney's Office should consult with the Professional Responsibility Advisory Office.

2. Use of Classified Investigative Technologies

Inappropriate use of classified investigative technologies may risk the compromise of such technologies. Hence, in an investigation relating to activities in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence, the use of such technologies must be in conformity with the Procedures for the Use of Classified Investigative Technologies in Criminal Cases.

C. OTHERWISE ILLEGAL ACTIVITY

1. Otherwise illegal activity by an FBI agent or employee in an undercover operation relating to activity in violation of federal criminal law that does not concern a threat to the national security or foreign intelligence must be approved in conformity with the Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations. Approval of otherwise illegal activity in conformity with those guidelines is sufficient and satisfies any approval requirement that would otherwise apply under these Guidelines.
2. Otherwise illegal activity by a human source must be approved in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
3. Otherwise illegal activity by an FBI agent or employee that is not within the scope of paragraph 1. must be approved by a United States Attorney's Office or a Department of Justice Division, except that a Special Agent in Charge may authorize the following:
 - a. otherwise illegal activity that would not be a felony under federal, state, local, or tribal law;
 - b. consensual monitoring of communications, even if a crime under state, local, or tribal law;
 - c. the controlled purchase, receipt, delivery, or sale of drugs, stolen property, or other contraband;
 - d. the payment of bribes;
 - e. the making of false representations in concealment of personal identity or the true ownership of a proprietary; and
 - f. conducting a money laundering transaction or transactions involving an aggregate amount not exceeding \$1 million.

However, in an investigation relating to a threat to the national security or foreign intelligence collection, a Special Agent in Charge may not authorize an activity that may constitute a violation of export control laws or laws that concern the proliferation of weapons of mass destruction. In such an investigation, a Special Agent in Charge may authorize an activity that may otherwise violate prohibitions of material support to terrorism only in accordance with standards established by the Director of the FBI and agreed to by the Assistant Attorney General for National Security.

4. The following activities may not be authorized:
 - a. Acts of violence.
 - b. Activities whose authorization is prohibited by law, including unlawful investigative methods, such as illegal electronic surveillance or illegal searches.

Subparagraph a., however, does not limit the right of FBI agents or employees to engage in any lawful use of force, including the use of force in self-defense or defense of others or otherwise in the lawful discharge of their duties.

5. An agent or employee may engage in otherwise illegal activity that could be authorized under this Subpart without the authorization required by paragraph 3. if necessary to meet an immediate threat to the safety of persons or property or to the national security, or to prevent the compromise of an investigation or the loss of a significant investigative opportunity. In such a case, prior to engaging in the otherwise illegal activity, every effort should be made by the agent or employee to consult with the Special Agent in Charge, and by the Special Agent in Charge to consult with the United States Attorney's Office or appropriate Department of Justice Division where the authorization of that office or division would be required under paragraph 3., unless the circumstances preclude such consultation. Cases in which otherwise illegal activity occurs pursuant to this paragraph without the authorization required by paragraph 3. shall be reported as soon as possible to the Special Agent in Charge, and by the Special Agent in Charge to FBI Headquarters and to the United States Attorney's Office or appropriate Department of Justice Division.
6. In an investigation relating to a threat to the national security or foreign intelligence collection, the National Security Division is the approving component for otherwise illegal activity for which paragraph 3. requires approval beyond internal FBI approval. However, officials in other components may approve otherwise illegal activity in such investigations as authorized by the Assistant Attorney General for National Security.

VI. RETENTION AND SHARING OF INFORMATION

A. RETENTION OF INFORMATION

1. The FBI shall retain records relating to activities under these Guidelines in accordance with a records retention plan approved by the National Archives and Records Administration.
2. The FBI shall maintain a database or records system that permits, with respect to each predicated investigation, the prompt retrieval of the status of the investigation (open or closed), the dates of opening and closing, and the basis for the investigation.

B. INFORMATION SHARING GENERALLY

1. Permissive Sharing

Consistent with law and with any applicable agreements or understandings with other agencies concerning the dissemination of information they have provided, the FBI may disseminate information obtained or produced through activities under these Guidelines:

- a. within the FBI and to other components of the Department of Justice;
- b. to other federal, state, local, or tribal agencies if related to their responsibilities and, in relation to other Intelligence Community agencies, the determination whether the information is related to the recipient's responsibilities may be left to the recipient;
- c. to congressional committees as authorized by the Department of Justice Office of Legislative Affairs;
- d. to foreign agencies if the information is related to their responsibilities and the dissemination is consistent with the interests of the United States (including national security interests) and the FBI has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person;
- e. if the information is publicly available, does not identify United States persons, or is disseminated with the consent of the person whom it concerns;
- f. if the dissemination is necessary to protect the safety or security of persons or property, to protect against or prevent a crime or threat to the national

security, or to obtain information for the conduct of an authorized FBI investigation; or

- g. if dissemination of the information is otherwise permitted by the Privacy Act (5 U.S.C. 552a).

2. Required Sharing

The FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements.

C. INFORMATION RELATING TO CRIMINAL MATTERS

1. Coordination with Prosecutors

In an investigation relating to possible criminal activity in violation of federal law, the agent conducting the investigation shall maintain periodic written or oral contact with the appropriate federal prosecutor, as circumstances warrant and as requested by the prosecutor. When, during such an investigation, a matter appears arguably to warrant prosecution, the agent shall present the relevant facts to the appropriate federal prosecutor. Information on investigations that have been closed shall be available on request to a United States Attorney or his or her designee or an appropriate Department of Justice official.

2. Criminal Matters Outside FBI Jurisdiction

When credible information is received by an FBI field office concerning serious criminal activity not within the FBI's investigative jurisdiction, the field office shall promptly transmit the information or refer the complainant to a law enforcement agency having jurisdiction, except where disclosure would jeopardize an ongoing investigation, endanger the safety of an individual, disclose the identity of a human source, interfere with a human source's cooperation, or reveal legally privileged information. If full disclosure is not made for the reasons indicated, then, whenever feasible, the FBI field office shall make at least limited disclosure to a law enforcement agency or agencies having jurisdiction, and full disclosure shall be made as soon as the need for restricting disclosure is no longer present. Where full disclosure is not made to the appropriate law enforcement agencies within 180 days, the FBI field office shall promptly notify FBI Headquarters in writing of the facts and circumstances concerning the criminal activity. The FBI shall make periodic reports to the Deputy Attorney General on such nondisclosures and incomplete disclosures, in a form suitable to protect the identity of human sources.

3. Reporting of Criminal Activity

- a. When it appears that an FBI agent or employee has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall notify the United States Attorney's Office or an appropriate Department of Justice Division. When it appears that a human source has engaged in criminal activity in the course of an investigation under these Guidelines, the FBI shall proceed as provided in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources. When information concerning possible criminal activity by any other person appears in the course of an investigation under these Guidelines, the FBI shall initiate an investigation of the criminal activity if warranted, and shall proceed as provided in paragraph 1. or 2.
- b. The reporting requirements under this paragraph relating to criminal activity by FBI agents or employees or human sources do not apply to otherwise illegal activity that is authorized in conformity with these Guidelines or other Attorney General guidelines or to minor traffic offenses.

D. INFORMATION RELATING TO NATIONAL SECURITY AND FOREIGN INTELLIGENCE MATTERS

The general principle reflected in current laws and policies is that there is a responsibility to provide information as consistently and fully as possible to agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. The FBI's responsibilities in this area include carrying out the requirements of the Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003), or any successor memorandum of understanding or agreement. Specific requirements also exist for internal coordination and consultation with other Department of Justice components, and for provision of national security and foreign intelligence information to White House agencies, as provided in the ensuing paragraphs.

1. Department of Justice

- a. The National Security Division shall have access to all information obtained by the FBI through activities relating to threats to the national security or foreign intelligence. The Director of the FBI and the Assistant Attorney General for National Security shall consult concerning these activities whenever requested by either of them, and the FBI shall provide such reports and information concerning these activities as the Assistant

Attorney General for National Security may request. In addition to any reports or information the Assistant Attorney General for National Security may specially request under this subparagraph, the FBI shall provide annual reports to the National Security Division concerning its foreign intelligence collection program, including information concerning the scope and nature of foreign intelligence collection activities in each FBI field office.

- b. The FBI shall keep the National Security Division apprised of all information obtained through activities under these Guidelines that is necessary to the ability of the United States to investigate or protect against threats to the national security, which shall include regular consultations between the FBI and the National Security Division to exchange advice and information relevant to addressing such threats through criminal prosecution or other means.
- c. Subject to subparagraphs d. and e., relevant United States Attorneys' Offices shall have access to and shall receive information from the FBI relating to threats to the national security, and may engage in consultations with the FBI relating to such threats, to the same extent as the National Security Division. The relevant United States Attorneys' Offices shall receive such access and information from the FBI field offices.
- d. In a counterintelligence investigation – i.e., an investigation relating to a matter described in Part VII.S.2 of these Guidelines – the FBI's provision of information to and consultation with a United States Attorney's Office are subject to authorization by the National Security Division. In consultation with the Executive Office for United States Attorneys and the FBI, the National Security Division shall establish policies setting forth circumstances in which the FBI will consult with the National Security Division prior to informing relevant United States Attorneys' Offices about such an investigation. The policies established by the National Security Division under this subparagraph shall (among other things) provide that:
 - i. the National Security Division will, within 30 days, authorize the FBI to share with the United States Attorneys' Offices information relating to certain espionage investigations, as defined by the policies, unless such information is withheld because of substantial national security considerations; and
 - ii. the FBI may consult freely with United States Attorneys' Offices concerning investigations within the scope of this subparagraph during an emergency, so long as the National Security Division is

notified of such consultation as soon as practical after the consultation.

- e. Information shared with a United States Attorney's Office pursuant to subparagraph c. or d. shall be disclosed only to the United States Attorney or any Assistant United States Attorneys designated by the United States Attorney as points of contact to receive such information. The United States Attorneys and designated Assistant United States Attorneys shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from the Foreign Intelligence Surveillance Act, including training concerning the secure handling and storage of such information and training concerning requirements and limitations relating to the use, retention, and dissemination of such information.
- f. The disclosure and sharing of information by the FBI under this paragraph is subject to any limitations required in orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. The disclosure and sharing of information by the FBI under this paragraph that may disclose the identity of human sources is governed by the relevant provisions of the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

2. White House

In order to carry out their responsibilities, the President, the Vice President, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security Affairs, the National Security Council and its staff, the Homeland Security Council and its staff, and other White House officials and offices require information from all federal agencies, including foreign intelligence, and information relating to international terrorism and other threats to the national security. The FBI accordingly may disseminate to the White House foreign intelligence and national security information obtained through activities under these Guidelines, subject to the following standards and procedures:

- a. Requests to the FBI for such information from the White House shall be made through the National Security Council staff or Homeland Security Council staff including, but not limited to, the National Security Council Legal and Intelligence Directorates and Office of Combating Terrorism, or through the President's Intelligence Advisory Board or the Counsel to the President.

- b. Compromising information concerning domestic officials or political organizations, or information concerning activities of United States persons intended to affect the political process in the United States, may be disseminated to the White House only with the approval of the Attorney General, based on a determination that such dissemination is needed for foreign intelligence purposes, for the purpose of protecting against international terrorism or other threats to the national security, or for the conduct of foreign affairs. However, such approval is not required for dissemination to the White House of information concerning efforts of foreign intelligence services to penetrate the White House, or concerning contacts by White House personnel with foreign intelligence service personnel.
- c. Examples of types of information that are suitable for dissemination to the White House on a routine basis include, but are not limited to:
 - i. information concerning international terrorism;
 - ii. information concerning activities of foreign intelligence services in the United States;
 - iii. information indicative of imminent hostilities involving any foreign power;
 - iv. information concerning potential cyber threats to the United States or its allies;
 - v. information indicative of policy positions adopted by foreign officials, governments, or powers, or their reactions to United States foreign policy initiatives;
 - vi. information relating to possible changes in leadership positions of foreign governments, parties, factions, or powers;
 - vii. information concerning foreign economic or foreign political matters that might have national security ramifications; and
 - viii. information set forth in regularly published national intelligence requirements.
- d. Communications by the FBI to the White House that relate to a national security matter and concern a litigation issue for a specific pending case must be made known to the Office of the Attorney General, the Office of

the Deputy Attorney General, or the Office of the Associate Attorney General. White House policy may specially limit or prescribe the White House personnel who may request information concerning such issues from the FBI.

- e. The limitations on dissemination of information by the FBI to the White House under these Guidelines do not apply to dissemination to the White House of information acquired in the course of an FBI investigation requested by the White House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

3. Special Statutory Requirements

- a. Dissemination of information acquired under the Foreign Intelligence Surveillance Act is, to the extent provided in that Act, subject to minimization procedures and other requirements specified in that Act.
- b. Information obtained through the use of National Security Letters under 15 U.S.C. 1681v may be disseminated in conformity with the general standards of this Part. Information obtained through the use of National Security Letters under other statutes may be disseminated in conformity with the general standards of this Part, subject to any applicable limitations in their governing statutory provisions: 12 U.S.C. 3414(a)(5)(B); 15 U.S.C. 1681u(f); 18 U.S.C. 2709(d); 50 U.S.C. 436(e).

VII. DEFINITIONS

- A. **CONSENSUAL MONITORING:** monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.
- B. **EMPLOYEE:** an FBI employee or an employee of another agency working under the direction and control of the FBI.
- C. **FOR OR ON BEHALF OF A FOREIGN POWER:** the determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in:
 - 1. control or policy direction;
 - 2. financial or material support; or
 - 3. leadership, assignments, or discipline.
- D. **FOREIGN COMPUTER INTRUSION:** the use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more U.S.-based computers.
- E. **FOREIGN INTELLIGENCE:** information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.
- F. **FOREIGN INTELLIGENCE REQUIREMENTS:**
 - 1. national intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
 - 2. requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
 - 3. directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.
- G. **FOREIGN POWER:**
 - 1. a foreign government or any component thereof, whether or not recognized by the United States;

2. a faction of a foreign nation or nations, not substantially composed of United States persons;
 3. an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
 4. a group engaged in international terrorism or activities in preparation therefor;
 5. a foreign-based political organization, not substantially composed of United States persons; or
 6. an entity that is directed or controlled by a foreign government or governments.
- H. HUMAN SOURCE: a Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.
- I. INTELLIGENCE ACTIVITIES: any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.
- J. INTERNATIONAL TERRORISM:
- Activities that:
1. involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction;
 2. appear to be intended:
 - i. to intimidate or coerce a civilian population;
 - ii. to influence the policy of a government by intimidation or coercion; or
 - iii. to affect the conduct of a government by assassination or kidnapping; and
 3. occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
- K. PROPRIETARY: a sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

- L. **PUBLICLY AVAILABLE:** information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.
- M. **RECORDS:** any records, databases, files, indices, information systems, or other retained information.
- N. **SENSITIVE INVESTIGATIVE MATTER:** an investigative matter involving the activities of a domestic public official or political candidate (involving corruption or a threat to the national security), religious or political organization or individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.
- O. **SENSITIVE MONITORING CIRCUMSTANCE:**
1. investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
 2. investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
 3. a party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
 4. the Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.
- P. **SPECIAL AGENT IN CHARGE:** the Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.
- Q. **SPECIAL EVENTS MANAGEMENT:** planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

- R. STATE, LOCAL, OR TRIBAL: any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.
- S. THREAT TO THE NATIONAL SECURITY:
1. international terrorism;
 2. espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons;
 3. foreign computer intrusion; and
 4. other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.
- T. UNITED STATES: when used in a geographic sense, means all areas under the territorial sovereignty of the United States.
- U. UNITED STATES PERSON:

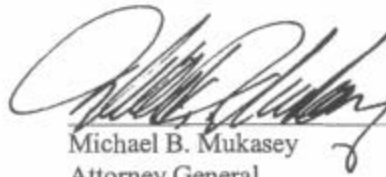
Any of the following, but not including any association or corporation that is a foreign power as defined in Subpart G.1.-.3.:

1. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;
2. an unincorporated association substantially composed of individuals who are United States persons; or
3. a corporation incorporated in the United States.

In applying paragraph 2., if a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of United States persons. If, however, the U.S.-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of United States persons. A classified directive provides further guidance concerning the determination of United States person status.

- V. USE: when used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

Date: 9/29/08



Michael B. Mukasey
Attorney General

APPENDIX B: (U) EXECUTIVE ORDER 12333

EXECUTIVE ORDER
12333
- - - - -

UNITED STATES INTELLIGENCE ACTIVITIES
DECEMBER 4, 1981
(AS AMENDED BY EXECUTIVE ORDERS 13284 (2003), 13355 (2004)
AND 13470 (2008))

PREAMBLE

Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible. For that purpose, by virtue of the authority vested in me by the Constitution and the laws of the United States of America, including the National Security Act of 1947, as amended, (Act) and as President of the United States of America, in order to provide for the effective conduct of United States intelligence activities and the protection of constitutional rights, it is hereby ordered as follows:

PART 1 Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Efforts

1.1 Goals. The United States intelligence effort shall provide the President, the National Security Council, and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.

(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its

interests.

(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.

(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President.

(d) Special emphasis should be given to detecting and countering:

- (1) Espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
- (2) Threats to the United States and its interests from terrorism; and
- (3) Threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.

(e) Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on all appropriate sources of information, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.

(f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector

entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

(g) All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance.

1.2 *The National Security Council.*

(a) *Purpose.* The National Security Council (NSC) shall act as the highest ranking executive branch entity that provides support to the President for review of, guidance for, and direction to the conduct of all foreign intelligence, counterintelligence, and covert action, and attendant policies and programs.

(b) *Covert Action and Other Sensitive Intelligence Operations.* The NSC shall consider and submit to the President a policy recommendation, including all dissents, on each proposed covert action and conduct a periodic review of ongoing covert action activities, including an evaluation of the effectiveness and consistency with current national policy of such activities and consistency with applicable legal requirements. The NSC shall perform such other functions related to covert action as the President may direct, but shall not undertake the conduct of covert actions. The NSC shall also review proposals for other sensitive intelligence operations.

1.3 *Director of National Intelligence.* Subject to the authority, direction, and control of the President, the Director of National Intelligence (Director) shall serve as the head of the Intelligence Community, act as the principal adviser to the President, to the NSC, and to the Homeland Security Council for intelligence matters related to national security, and shall oversee and direct the implementation of the National Intelligence Program and execution of the National Intelligence

Program budget. The Director will lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall, in carrying out the duties and responsibilities under this section, take into account the views of the heads of departments containing an element of the Intelligence Community and of the Director of the Central Intelligence Agency.

(a) Except as otherwise directed by the President or prohibited by law, the Director shall have access to all information and intelligence described in section 1.5(a) of this order. For the purpose of access to and sharing of information and intelligence, the Director:

(1) Is hereby assigned the function under section 3(5) of the Act, to determine that intelligence, regardless of the source from which derived and including information gathered within or outside the United States, pertains to more than one United States Government agency; and

(2) Shall develop guidelines for how information or intelligence is provided to or accessed by the Intelligence Community in accordance with section 1.5(a) of this order, and for how the information or intelligence may be used and shared by the Intelligence Community. All guidelines developed in accordance with this section shall be approved by the Attorney General and, where applicable, shall be consistent with guidelines issued pursuant to section 1016 of the Intelligence Reform and Terrorism Protection Act of 2004 (Public Law 108-458) (IRTPA).

(b) In addition to fulfilling the obligations and responsibilities prescribed by the Act, the Director:

(1) Shall establish objectives, priorities, and guidance for the Intelligence Community to ensure timely and effective collection, processing, analysis, and dissemination of intelligence, of whatever nature and from whatever source

derived;

(2) May designate, in consultation with affected heads of departments or Intelligence Community elements, one or more Intelligence Community elements to develop and to maintain services of common concern on behalf of the Intelligence Community if the Director determines such services can be more efficiently or effectively accomplished in a consolidated manner;

(3) Shall oversee and provide advice to the President and the NSC with respect to all ongoing and proposed covert action programs;

(4) In regard to the establishment and conduct of intelligence arrangements and agreements with foreign governments and international organizations:

(A) May enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations;

(B) Shall formulate policies concerning intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations; and

(C) Shall align and synchronize intelligence and counterintelligence foreign relationships among the elements of the Intelligence Community to further United States national security, policy, and intelligence objectives;

(5) Shall participate in the development of procedures approved by the Attorney General governing criminal drug intelligence activities abroad to ensure that these activities are consistent with foreign intelligence programs;

(6) Shall establish common security and access standards for managing and handling intelligence systems, information, and products, with special emphasis on facilitating:

(A) The fullest and most prompt access to and dissemination of information and intelligence practicable, assigning the highest priority to detecting, preventing, preempting, and disrupting terrorist threats and activities against the United States, its interests, and allies; and

(B) The establishment of standards for an interoperable information sharing enterprise that facilitates the sharing of intelligence information among elements of the Intelligence Community;

(7) Shall ensure that appropriate departments and agencies have access to intelligence and receive the support needed to perform independent analysis;

(8) Shall protect, and ensure that programs are developed to protect, intelligence sources, methods, and activities from unauthorized disclosure;

(9) Shall, after consultation with the heads of affected departments and agencies, establish guidelines for Intelligence Community elements for:

(A) Classification and declassification of all intelligence and intelligence-related information classified under the authority of the Director or the authority of the head of a department or Intelligence Community element; and

(B) Access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered, to include intelligence originally classified by the head of a department or Intelligence Community element, except that access to and dissemination of information concerning United States persons shall be governed by procedures developed in accordance with Part 2 of this order;

(10) May, only with respect to Intelligence Community elements, and after consultation with the head of the

originating Intelligence Community element or the head of the originating department, declassify, or direct the declassification of, information or intelligence relating to intelligence sources, methods, and activities. The Director may only delegate this authority to the Principal Deputy Director of National Intelligence;

(11) May establish, operate, and direct one or more national intelligence centers to address intelligence priorities;

(12) May establish Functional Managers and Mission Managers, and designate officers or employees of the United States to serve in these positions.

(A) Functional Managers shall report to the Director concerning the execution of their duties as Functional Managers, and may be charged with developing and implementing strategic guidance, policies, and procedures for activities related to a specific intelligence discipline or set of intelligence activities; set training and tradecraft standards; and ensure coordination within and across intelligence disciplines and Intelligence Community elements and with related non-intelligence activities. Functional Managers may also advise the Director on: the management of resources; policies and procedures; collection capabilities and gaps; processing and dissemination of intelligence; technical architectures; and other issues or activities determined by the Director.

(i) The Director of the National Security Agency is designated the Functional Manager for signals intelligence;

(ii) The Director of the Central Intelligence Agency is designated the Functional Manager for human intelligence; and

(iii) The Director of the National

Geospatial-Intelligence Agency is designated the Functional Manager for geospatial intelligence.

(B) Mission Managers shall serve as principal substantive advisors on all or specified aspects of intelligence related to designated countries, regions, topics, or functional issues;

(13) Shall establish uniform criteria for the determination of relative priorities for the transmission of critical foreign intelligence, and advise the Secretary of Defense concerning the communications requirements of the Intelligence Community for the transmission of such communications;

(14) Shall have ultimate responsibility for production and dissemination of intelligence produced by the Intelligence Community and authority to levy analytic tasks on intelligence production organizations within the Intelligence Community, in consultation with the heads of the Intelligence Community elements concerned;

(15) May establish advisory groups for the purpose of obtaining advice from within the Intelligence Community to carry out the Director's responsibilities, to include Intelligence Community executive management committees composed of senior Intelligence Community leaders. Advisory groups shall consist of representatives from elements of the Intelligence Community, as designated by the Director, or other executive branch departments, agencies, and offices, as appropriate;

(16) Shall ensure the timely exploitation and dissemination of data gathered by national intelligence collection means, and ensure that the resulting intelligence is disseminated immediately to appropriate government elements, including military commands;

(17) Shall determine requirements and priorities

for, and manage and direct the tasking, collection, analysis, production, and dissemination of, national intelligence by elements of the Intelligence Community, including approving requirements for collection and analysis and resolving conflicts in collection requirements and in the tasking of national collection assets of Intelligence Community elements (except when otherwise directed by the President or when the Secretary of Defense exercises collection tasking authority under plans and arrangements approved by the Secretary of Defense and the Director);

(18) May provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community; and shall establish

procedures, in consultation with affected heads of departments or agencies and subject to approval by the Attorney General, to implement this authority and to monitor or evaluate the responsiveness of United States Government departments, agencies, and other establishments;

(19) Shall fulfill the responsibilities in section 1.3(b)(17) and (18) of this order, consistent with applicable law and with full consideration of the rights of United States persons, whether information is to be collected inside or outside the United States;

(20) Shall ensure, through appropriate policies and procedures, the deconfliction, coordination, and integration of all intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program. In accordance with these policies and procedures:

(A) The Director of the Federal Bureau of

Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;

(B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

(C) All policies and procedures for the coordination of counterintelligence activities and the clandestine collection of foreign intelligence inside the United States shall be subject to the approval of the Attorney General; and

(D) All policies and procedures developed under this section shall be coordinated with the heads of affected departments and Intelligence Community elements;

(21) Shall, with the concurrence of the heads of affected departments and agencies, establish joint procedures to deconflict, coordinate, and synchronize intelligence activities conducted by an Intelligence Community element or funded by the National Intelligence Program, with intelligence activities, activities that involve foreign intelligence and security services, or activities that involve the use of clandestine methods, conducted by other United States Government departments, agencies, and establishments;

(22) Shall, in coordination with the heads of departments containing elements of the Intelligence Community, develop procedures to govern major system acquisitions funded in whole or in majority part by the National Intelligence Program;

(23) Shall seek advice from the Secretary of State to ensure that the foreign policy implications of proposed

intelligence activities are considered, and shall ensure, through appropriate policies and procedures, that intelligence activities are conducted in a manner consistent with the responsibilities pursuant to law and presidential direction of Chiefs of United States Missions; and

(24) Shall facilitate the use of Intelligence Community products by the Congress in a secure manner.

(c) The Director's exercise of authorities in the Act and this order shall not abrogate the statutory or other responsibilities of the heads of departments of the United States Government or the Director of the Central Intelligence Agency. Directives issued and actions taken by the Director in the exercise of the Director's authorities and responsibilities to integrate, coordinate, and make the Intelligence Community more effective in providing intelligence related to national security shall be implemented by the elements of the Intelligence Community, provided that any department head whose department contains an element of the Intelligence Community and who believes that a directive or action of the Director violates the requirements of section 1018 of the IRTPA or this subsection shall bring the issue to the attention of the Director, the NSC, or the President for resolution in a manner that respects and does not abrogate the statutory responsibilities of the heads of the departments.

(d) Appointments to certain positions.

(1) The relevant department or bureau head shall provide recommendations and obtain the concurrence of the Director for the selection of: the Director of the National Security Agency, the Director of the National Reconnaissance Office, the Director of the National Geospatial-Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State for

Intelligence and Research, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury, and the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation. If the Director does not concur in the recommendation, the department head may not fill the vacancy or make the recommendation to the President, as the case may be. If the department head and the Director do not reach an agreement on the selection or recommendation, the Director and the department head concerned may advise the President directly of the Director's intention to withhold concurrence.

(2) The relevant department head shall consult with the Director before appointing an individual to fill a vacancy or recommending to the President an individual be nominated to fill a vacancy in any of the following positions: the Under Secretary of Defense for Intelligence; the Director of the Defense Intelligence Agency; uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps above the rank of Major General or Rear Admiral; the Assistant Commandant of the Coast Guard for Intelligence; and the Assistant Attorney General for National Security.

(e) Removal from certain positions.

(1) Except for the Director of the Central Intelligence Agency, whose removal the Director may recommend to the President, the Director and the relevant department head shall consult on the removal, or recommendation to the President for removal, as the case may be, of: the Director of the National Security Agency, the Director of the National Geospatial-Intelligence Agency, the Director of the Defense Intelligence Agency, the Under Secretary of Homeland Security for Intelligence and Analysis, the Assistant Secretary of State

for Intelligence and Research, and the Assistant Secretary for Intelligence and Analysis of the Department of the Treasury. If the Director and the department head do not agree on removal, or recommendation for removal, either may make a recommendation to the President for the removal of the individual.

(2) The Director and the relevant department or bureau head shall consult on the removal of: the Executive Assistant Director for the National Security Branch of the Federal Bureau of Investigation, the Director of the Office of Intelligence and Counterintelligence of the Department of Energy, the Director of the National Reconnaissance Office, the Assistant Commandant of the Coast Guard for Intelligence, and the Under Secretary of Defense for Intelligence. With respect to an individual appointed by a department head, the department head may remove the individual upon the request of the Director; if the department head chooses not to remove the individual, either the Director or the department head may advise the President of the department head's intention to retain the individual. In the case of the Under Secretary of Defense for Intelligence, the Secretary of Defense may recommend to the President either the removal or the retention of the individual. For uniformed heads of the intelligence elements of the Army, the Navy, the Air Force, and the Marine Corps, the Director may make a recommendation for removal to the Secretary of Defense.

(3) Nothing in this subsection shall be construed to limit or otherwise affect the authority of the President to nominate, appoint, assign, or terminate the appointment or assignment of any individual, with or without a consultation, recommendation, or concurrence.

1.4 *The Intelligence Community.* Consistent with applicable Federal law and with the other provisions of this order, and

under the leadership of the Director, as specified in such law and this order, the Intelligence Community shall:

(a) Collect and provide information needed by the President and, in the performance of executive functions, the Vice President, the NSC, the Homeland Security Council, the Chairman of the Joint Chiefs of Staff, senior military commanders, and other executive branch officials and, as appropriate, the Congress of the United States;

(b) In accordance with priorities set by the President, collect information concerning, and conduct activities to protect against, international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents;

(c) Analyze, produce, and disseminate intelligence;

(d) Conduct administrative, technical, and other support activities within the United States and abroad necessary for the performance of authorized activities, to include providing services of common concern for the Intelligence Community as designated by the Director in accordance with this order;

(e) Conduct research, development, and procurement of technical systems and devices relating to authorized functions and missions or the provision of services of common concern for the Intelligence Community;

(f) Protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Intelligence Community elements as are necessary;

(g) Take into account State, local, and tribal governments' and, as appropriate, private sector entities' information needs relating to national and homeland security;

(h) Deconflict, coordinate, and integrate all intelligence activities and other information gathering in accordance with section 1.3(b) (20) of this order; and

(i) Perform such other functions and duties related to intelligence activities as the President may direct.

1.5 Duties and Responsibilities of the Heads of Executive Branch Departments and Agencies. The heads of all departments and agencies shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Provide all programmatic and budgetary information necessary to support the Director in developing the National Intelligence Program;

(c) Coordinate development and implementation of intelligence systems and architectures and, as appropriate, operational systems and architectures of their departments, agencies, and other elements with the Director to respond to national intelligence requirements and all applicable information sharing and security guidelines, information privacy, and other legal requirements;

(d) Provide, to the maximum extent permitted by law, subject to the availability of appropriations and not inconsistent with the mission of the department or agency, such further support to the Director as the Director may request,

after consultation with the head of the department or agency, for the performance of the Director's functions;

(e) Respond to advisory tasking from the Director under section 1.3(b) (18) of this order to the greatest extent possible, in accordance with applicable policies established by the head of the responding department or agency;

(f) Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions;

(g) Deconflict, coordinate, and integrate all intelligence activities in accordance with section 1.3(b) (20), and intelligence and other activities in accordance with section 1.3(b) (21) of this order;

(h) Inform the Attorney General, either directly or through the Federal Bureau of Investigation, and the Director of clandestine collection of foreign intelligence and counterintelligence activities inside the United States not coordinated with the Federal Bureau of Investigation;

(i) Pursuant to arrangements developed by the head of the department or agency and the Director of the Central Intelligence Agency and approved by the Director, inform the Director and the Director of the Central Intelligence Agency, either directly or through his designee serving outside the United States, as appropriate, of clandestine collection of foreign intelligence collected through human sources or through human-enabled means outside the United States that has not been coordinated with the Central Intelligence Agency; and

(j) Inform the Secretary of Defense, either directly or through his designee, as appropriate, of clandestine collection of foreign intelligence outside the United States in a region of

combat or contingency military operations designated by the Secretary of Defense, for purposes of this paragraph, after consultation with the Director of National Intelligence.

1.6 *Heads of Elements of the Intelligence Community.* The heads of elements of the Intelligence Community shall:

(a) Provide the Director access to all information and intelligence relevant to the national security or that otherwise is required for the performance of the Director's duties, to include administrative and other appropriate management information, except such information excluded by law, by the President, or by the Attorney General acting under this order at the direction of the President;

(b) Report to the Attorney General possible violations of Federal criminal laws by employees and of specified Federal criminal laws by any other person as provided in procedures agreed upon by the Attorney General and the head of the department, agency, or establishment concerned, in a manner consistent with the protection of intelligence sources and methods, as specified in those procedures;

(c) Report to the Intelligence Oversight Board, consistent with Executive Order 13462 of February 29, 2008, and provide copies of all such reports to the Director, concerning any intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive;

(d) Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure in accordance with guidance from the Director;

(e) Facilitate, as appropriate, the sharing of information or intelligence, as directed by law or the President, to State, local, tribal, and private sector entities;

(f) Disseminate information or intelligence to foreign

governments and international organizations under intelligence or counterintelligence arrangements or agreements established in accordance with section 1.3(b)(4) of this order;

(g) Participate in the development of procedures approved by the Attorney General governing production and dissemination of information or intelligence resulting from criminal drug intelligence activities abroad if they have intelligence responsibilities for foreign or domestic criminal drug production and trafficking; and

(h) Ensure that the inspectors general, general counsels, and agency officials responsible for privacy or civil liberties protection for their respective organizations have access to any information or intelligence necessary to perform their official duties.

1.7 *Intelligence Community Elements.* Each element of the Intelligence Community shall have the duties and responsibilities specified below, in addition to those specified by law or elsewhere in this order. Intelligence Community elements within executive departments shall serve the information and intelligence needs of their respective heads of departments and also shall operate as part of an integrated Intelligence Community, as provided in law or this order.

(a) THE CENTRAL INTELLIGENCE AGENCY. The Director of the Central Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence;

(2) Conduct counterintelligence activities without assuming or performing any internal security functions within the United States;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for

cover and proprietary arrangements;

(4) Conduct covert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective;

(5) Conduct foreign intelligence liaison relationships with intelligence or security services of foreign governments or international organizations consistent with section 1.3(b)(4) of this order;

(6) Under the direction and guidance of the Director, and in accordance with section 1.3(b)(4) of this order, coordinate the implementation of intelligence and counterintelligence relationships between elements of the Intelligence Community and the intelligence or security services of foreign governments or international organizations; and

(7) Perform such other functions and duties related to intelligence as the Director may direct.

(b) THE DEFENSE INTELLIGENCE AGENCY. The Director of the Defense Intelligence Agency shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions;

(2) Collect, analyze, produce, or, through tasking and coordination, provide defense and defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other Defense components, and non-Defense agencies;

(3) Conduct counterintelligence activities;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover and proprietary arrangements;

(5) Conduct foreign defense intelligence liaison relationships and defense intelligence exchange programs with foreign defense establishments, intelligence or security services of foreign governments, and international organizations in accordance with sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order;

(6) Manage and coordinate all matters related to the Defense Attaché system; and

(7) Provide foreign intelligence and counterintelligence staff support as directed by the Secretary of Defense.

(c) THE NATIONAL SECURITY AGENCY. The Director of the National Security Agency shall:

(1) Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Establish and operate an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense, after coordination with the Director;

(3) Control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the

direct support of military commanders;

(4) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements;

(5) Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

(6) Act as the National Manager for National Security Systems as established in law and policy, and in this capacity be responsible to the Secretary of Defense and to the Director;

(7) Prescribe, consistent with section 102A(g) of the Act, within its field of authorized operations, security regulations covering operating practices, including the transmission, handling, and distribution of signals intelligence and communications security material within and among the elements under control of the Director of the National Security Agency, and exercise the necessary supervisory control to ensure compliance with the regulations; and

(8) Conduct foreign cryptologic liaison relationships in accordance with sections 1.3(b) (4), 1.7(a) (6), and 1.10(i) of this order.

(d) THE NATIONAL RECONNAISSANCE OFFICE. The Director of the National Reconnaissance Office shall:

(1) Be responsible for research and development, acquisition, launch, deployment, and operation of overhead systems and related data processing facilities to collect intelligence and information to support national and departmental missions and other United States Government needs; and

(2) Conduct foreign liaison relationships relating to the above missions, in accordance with sections 1.3(b) (4), 1.7(a) (6), and 1.10(i) of this order.

(e) THE NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. The Director of the National Geospatial-Intelligence Agency shall:

(1) Collect, process, analyze, produce, and disseminate geospatial intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;

(2) Provide geospatial intelligence support for national and departmental requirements and for the conduct of military operations;

(3) Conduct administrative and technical support activities within and outside the United States as necessary for cover arrangements; and

(4) Conduct foreign geospatial intelligence liaison relationships, in accordance with sections 1.3(b) (4), 1.7(a) (6), and 1.10(i) of this order.

(f) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE ARMY, NAVY, AIR FORCE, AND MARINE CORPS. The Commanders and heads of the intelligence and counterintelligence elements of the Army, Navy, Air Force, and Marine Corps shall:

(1) Collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations in accordance with

sections 1.3(b)(4), 1.7(a)(6), and 1.10(i) of this order.

(g) INTELLIGENCE ELEMENTS OF THE FEDERAL BUREAU OF INVESTIGATION. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the intelligence elements of the Federal Bureau of Investigation shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions, in accordance with procedural guidelines approved by the Attorney General, after consultation with the Director;

(2) Conduct counterintelligence activities; and

(3) Conduct foreign intelligence and counterintelligence liaison relationships with intelligence, security, and law enforcement services of foreign governments or international organizations in accordance with sections 1.3(b)(4) and 1.7(a)(6) of this order.

(h) THE INTELLIGENCE AND COUNTERINTELLIGENCE ELEMENTS OF THE COAST GUARD. The Commandant of the Coast Guard shall:

(1) Collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions;

(2) Conduct counterintelligence activities;

(3) Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities; and

(4) Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international

organizations in accordance with sections 1.3(b) (4), 1.7(a) (6), and, when operating as part of the Department of Defense, 1.10(i) of this order.

(i) THE BUREAU OF INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF THE TREASURY; THE OFFICE OF NATIONAL SECURITY INTELLIGENCE, DRUG ENFORCEMENT ADMINISTRATION; THE OFFICE OF INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY; AND THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE, DEPARTMENT OF ENERGY.

The heads of the Bureau of Intelligence and Research, Department of State; the Office of Intelligence and Analysis, Department of the Treasury; the Office of National Security Intelligence, Drug Enforcement Administration; the Office of Intelligence and Analysis, Department of Homeland Security; and the Office of Intelligence and Counterintelligence, Department of Energy shall:

(1) Collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions; and

(2) Conduct and participate in analytic or information exchanges with foreign partners and international organizations in accordance with sections 1.3(b) (4) and 1.7(a) (6) of this order.

(j) THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. The Director shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support the missions of the Office of the Director of National Intelligence, including the National Counterterrorism Center, and to support other national missions.

1.8 The Department of State. In addition to the authorities

exercised by the Bureau of Intelligence and Research under sections 1.4 and 1.7(i) of this order, the Secretary of State shall:

- (a) Collect (overtly or through publicly available sources) information relevant to United States foreign policy and national security concerns;
- (b) Disseminate, to the maximum extent possible, reports received from United States diplomatic and consular posts;
- (c) Transmit reporting requirements and advisory taskings of the Intelligence Community to the Chiefs of United States Missions abroad; and
- (d) Support Chiefs of United States Missions in discharging their responsibilities pursuant to law and presidential direction.

1.9 *The Department of the Treasury.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of the Treasury under sections 1.4 and 1.7(i) of this order the Secretary of the Treasury shall collect (overtly or through publicly available sources) foreign financial information and, in consultation with the Department of State, foreign economic information.

1.10 *The Department of Defense.* The Secretary of Defense shall:

- (a) Collect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director;
- (b) Collect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities;
- (c) Conduct programs and missions necessary to fulfill

national, departmental, and tactical intelligence requirements;

(d) Conduct counterintelligence activities in support of Department of Defense components and coordinate counterintelligence activities in accordance with section 1.3(b) (20) and (21) of this order;

(e) Act, in coordination with the Director, as the executive agent of the United States Government for signals intelligence activities;

(f) Provide for the timely transmission of critical intelligence, as defined by the Director, within the United States Government;

(g) Carry out or contract for research, development, and procurement of technical systems and devices relating to authorized intelligence functions;

(h) Protect the security of Department of Defense installations, activities, information, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the Department of Defense as are necessary;

(i) Establish and maintain defense intelligence relationships and defense intelligence exchange programs with selected cooperative foreign defense establishments, intelligence or security services of foreign governments, and international organizations, and ensure that such relationships and programs are in accordance with sections 1.3(b) (4), 1.3(b) (21) and 1.7(a) (6) of this order;

(j) Conduct such administrative and technical support activities within and outside the United States as are necessary to provide for cover and proprietary arrangements, to perform the functions described in sections (a) through (i) above, and to support the Intelligence Community elements of the Department of

Defense; and

(k) Use the Intelligence Community elements within the Department of Defense identified in section 1.7(b) through (f) and, when the Coast Guard is operating as part of the Department of Defense,

(h) above to carry out the Secretary of Defense's responsibilities assigned in this section or other departments, agencies, or offices within the Department of Defense, as appropriate, to conduct the intelligence missions and responsibilities assigned to the Secretary of Defense.

1.11 *The Department of Homeland Security.* In addition to the authorities exercised by the Office of Intelligence and Analysis of the Department of Homeland Security under sections 1.4 and 1.7(i) of this order, the Secretary of Homeland Security shall conduct, through the United States Secret Service, activities to determine the existence and capability of surveillance equipment being used against the President or the Vice President of the United States, the Executive Office of the President, and, as authorized by the Secretary of Homeland Security or the President, other Secret Service protectees and United States officials. No information shall be acquired intentionally through such activities except to protect against use of such surveillance equipment, and those activities shall be conducted pursuant to procedures agreed upon by the Secretary of Homeland Security and the Attorney General.

1.12 *The Department of Energy.* In addition to the authorities exercised by the Office of Intelligence and Counterintelligence of the Department of Energy under sections 1.4 and 1.7(i) of this order, the Secretary of Energy shall:

(a) Provide expert scientific, technical, analytic, and research capabilities to other agencies within the Intelligence Community, as appropriate;

(b) Participate in formulating intelligence collection and analysis requirements where the special expert capability of the Department can contribute; and

(c) Participate with the Department of State in overtly collecting information with respect to foreign energy matters.

1.13 *The Federal Bureau of Investigation.* In addition to the authorities exercised by the intelligence elements of the Federal Bureau of Investigation of the Department of Justice under sections 1.4 and 1.7(g) of this order and under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Director of the Federal Bureau of Investigation shall provide technical assistance, within or outside the United States, to foreign intelligence and law enforcement services, consistent with section 1.3(b)(20) and (21) of this order, as may be necessary to support national or departmental missions.

PART 2 *Conduct of Intelligence Activities*

2.1 *Need.* Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents, is essential to informed decisionmaking in the areas of national security, national defense, and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative, and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the United States was founded.

2.2 *Purpose.* This Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities, the spread of weapons of mass destruction,

and espionage conducted by foreign powers. Set forth below are certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests. Nothing in this Order shall be construed to apply to or interfere with any authorized civil or criminal law enforcement responsibility of any department or agency.

2.3 *Collection of information.* Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

(a) Information that is publicly available or collected with the consent of the person concerned;

(b) Information constituting foreign intelligence or counterintelligence, including such information concerning corporations or other commercial organizations. Collection within the United States of foreign intelligence not otherwise obtainable shall be undertaken by the Federal Bureau of Investigation (FBI) or, when significant foreign intelligence is sought, by other authorized elements of the Intelligence Community, provided that no foreign intelligence collection by such elements may be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons;

(c) Information obtained in the course of a lawful foreign

intelligence, counterintelligence, international drug or international terrorism investigation;

(d) Information needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations;

(e) Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure. Collection within the United States shall be undertaken by the FBI except that other elements of the Intelligence Community may also collect such information concerning present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for such employment or contracting;

(f) Information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;

(g) Information arising out of a lawful personnel, physical, or communications security investigation;

(h) Information acquired by overhead reconnaissance not directed at specific United States persons;

(i) Incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws; and

(j) Information necessary for administrative purposes.

In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the

Director in coordination with the Secretary of Defense and approved by the Attorney General.

2.4 *Collection Techniques.* Elements of the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Elements of the Intelligence Community are not authorized to use such techniques as electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by the Attorney General, after consultation with the Director. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes. These procedures shall not authorize:

(a) The Central Intelligence Agency (CIA) to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance;

(b) Unconsented physical searches in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Searches by counterintelligence elements of the military services directed against military personnel within the United States or abroad for intelligence purposes, when authorized by a military commander empowered to approve physical searches for law enforcement purposes, based upon a finding of probable cause to believe that such persons are acting as agents of foreign powers; and

(2) Searches by CIA of personal property of non-United States persons lawfully in its possession;

(c) Physical surveillance of a United States person in the United States by elements of the Intelligence Community other than the FBI, except for:

(1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and

(2) Physical surveillance of a military person employed by a non-intelligence element of a military service; and

(d) Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

2.5 *Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power. The authority delegated pursuant to this paragraph, including the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act.

2.6 *Assistance to Law Enforcement and other Civil Authorities.* Elements of the Intelligence Community are authorized to:

(a) Cooperate with appropriate law enforcement agencies for the purpose of protecting the employees, information, property, and facilities of any element of the Intelligence Community;

(b) Unless otherwise precluded by law or this Order,

participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers, or international terrorist or narcotics activities;

(c) Provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency, or when lives are endangered, to support local law enforcement agencies. Provision of assistance by expert personnel shall be approved in each case by the general counsel of the providing element or department; and

(d) Render any other assistance and cooperation to law enforcement or other civil authorities not precluded by applicable law.

2.7 Contracting. Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution.

2.8 Consistency With Other Laws. Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.

2.9 Undisclosed Participation in Organizations Within the United States. No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation to appropriate officials of the organization, except in accordance with procedures established by the head of the Intelligence Community element concerned or the head of a department containing such element and approved by

the Attorney General, after consultation with the Director. Such participation shall be authorized only if it is essential to achieving lawful purposes as determined by the Intelligence Community element head or designee. No such participation may be undertaken for the purpose of influencing the activity of the organization or its members except in cases where:

(a) The participation is undertaken on behalf of the FBI in the course of a lawful investigation; or

(b) The organization concerned is composed primarily of individuals who are not United States persons and is reasonably believed to be acting on behalf of a foreign power.

2.10 *Human Experimentation.* No element of the Intelligence Community shall sponsor, contract for, or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines.

2.11 *Prohibition on Assassination.* No person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination.

2.12 *Indirect Participation.* No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this Order.

2.13 *Limitation on Covert Action.* No covert action may be conducted which is intended to influence United States political processes, public opinion, policies, or media.

PART 3 *General Provisions*

3.1 *Congressional Oversight.* The duties and responsibilities of the Director and the heads of other departments, agencies, elements, and entities engaged in intelligence activities to cooperate with the Congress in the conduct of its responsibilities for oversight of intelligence activities shall

be implemented in accordance with applicable law, including title V of the Act. The requirements of applicable law, including title V of the Act, shall apply to all covert action activities as defined in this Order.

3.2 Implementation. The President, supported by the NSC, and the Director shall issue such appropriate directives, procedures, and guidance as are necessary to implement this order. Heads of elements within the Intelligence Community shall issue appropriate procedures and supplementary directives consistent with this order. No procedures to implement Part 2 of this order shall be issued without the Attorney General's approval, after consultation with the Director. The Attorney General shall provide a statement of reasons for not approving any procedures established by the head of an element in the Intelligence Community (or the head of the department containing such element) other than the FBI. In instances where the element head or department head and the Attorney General are unable to reach agreements on other than constitutional or other legal grounds, the Attorney General, the head of department concerned, or the Director shall refer the matter to the NSC.

3.3 Procedures. The activities herein authorized that require procedures shall be conducted in accordance with existing procedures or requirements established under Executive Order 12333. New procedures, as required by Executive Order 12333, as further amended, shall be established as expeditiously as possible. All new procedures promulgated pursuant to Executive Order 12333, as amended, shall be made available to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

3.4 References and Transition. References to "Senior Officials of the Intelligence Community" or "SOICs" in executive orders or

other Presidential guidance, shall be deemed references to the heads of elements in the Intelligence Community, unless the President otherwise directs; references in Intelligence Community or Intelligence Community element policies or guidance, shall be deemed to be references to the heads of elements of the Intelligence Community, unless the President or the Director otherwise directs.

3.5 *Definitions.* For the purposes of this Order, the following terms shall have these meanings:

(a) *Counterintelligence* means information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

(b) *Covert action* means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include:

(1) Activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities, traditional activities to improve or maintain the operational security of United States Government programs, or administrative activities;

(2) Traditional diplomatic or military activities or routine support to such activities;

(3) Traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or

(4) Activities to provide routine support to the overt activities (other than activities described in

paragraph (1), (2), or (3)) of other United States Government agencies abroad.

(c) *Electronic surveillance* means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

(d) *Employee* means a person employed by, assigned or detailed to, or acting for an element within the Intelligence Community.

(e) *Foreign intelligence* means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

(f) *Intelligence* includes foreign intelligence and counterintelligence.

(g) *Intelligence activities* means all activities that elements of the Intelligence Community are authorized to conduct pursuant to this order.

(h) *Intelligence Community* and elements of the Intelligence Community refers to:

- (1) The Office of the Director of National Intelligence;
- (2) The Central Intelligence Agency;
- (3) The National Security Agency;
- (4) The Defense Intelligence Agency;
- (5) The National Geospatial-Intelligence Agency;
- (6) The National Reconnaissance Office;
- (7) The other offices within the Department

of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

(8) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps;

(9) The intelligence elements of the Federal Bureau of Investigation;

(10) The Office of National Security Intelligence of the Drug Enforcement Administration;

(11) The Office of Intelligence and Counterintelligence of the Department of Energy;

(12) The Bureau of Intelligence and Research of the Department of State;

(13) The Office of Intelligence and Analysis of the Department of the Treasury;

(14) The Office of Intelligence and Analysis of the Department of Homeland Security;

(15) The intelligence and counterintelligence elements of the Coast Guard; and

(16) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director and the head of the department or agency concerned, as an element of the Intelligence Community.

(i) *National Intelligence and Intelligence Related to National Security* means all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that pertains, as determined consistent with any guidance issued by the President, or that is determined for the purpose of access to information by the Director in accordance with section 1.3(a)(1) of this order, to pertain to more than one United States Government agency; and that involves threats to the United States, its

people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

(j) *The National Intelligence Program* means all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President. Such term does not include programs, projects, or activities of the military departments to acquire intelligence solely for the planning and conduct of tactical military operations by United States Armed Forces.

(k) *United States person* means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

3.6 *Revocation.* Executive Orders 13354 and 13355 of August 27, 2004, are revoked; and paragraphs 1.3(b) (9) and (10) of Part 1 supersede provisions within Executive Order 12958, as amended, to the extent such provisions in Executive Order 12958, as amended, are inconsistent with this Order.

3.7 *General Provisions.*

(a) Consistent with section 1.3(c) of this order, nothing in this order shall be construed to impair or otherwise affect:

- (1) Authority granted by law to a department or agency, or the head thereof; or
- (2) Functions of the Director of the Office of Management and Budget relating to budget, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.

/s/ Ronald Reagan

THE WHITE HOUSE

December 4, 1981

APPENDIX C: (U//FOUO) USE AND TARGETING OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI PREDICATED INVESTIGATION; INTERVIEW OF A FEDERAL PRISONER HELD IN THE CUSTODY OF THE BOP OR USMS DURING AN FBI ASSESSMENT OR PREDICATED INVESTIGATION

C.1 (U) OVERVIEW/SUMMARY

(U//FOUO) Use and Targeting a Federal Prisoner: During an FBI Predicated Investigation, it may be necessary and appropriate to: 1) use a cooperating federal prisoner to gather and obtain evidence and intelligence; or 2) target a federal prisoner. This policy sets forth the approval process for the use of and targeting of a federal prisoner held in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS).

(U//FOUO) Interview a Federal Prisoner: During an FBI Assessment or Predicated Investigation, it may be necessary and appropriate to interview a federal prisoner in the custody of the BOP or USMS. This policy sets forth the approval process for the interview of a federal prisoner held in the custody of the BOP or the USMS during an FBI Assessment or Predicated Investigation.

(U//FOUO) Exclusions from this Policy: This policy does not apply to:

- A) (U//FOUO) the use of a Federal Prisoner, who is a Confidential Human Source (CHS), under the circumstances listed in the CHSPM section 6.2.1; or
- B) (U//FOUO) the use, targeting, or interview of a prisoner held in the custody of the Department of Defense (DOD).

C.2 (U) LEGAL AUTHORITY

(U) The FBI is authorized by the Department of Justice (DOJ) to use and target a federal prisoner for investigative purposes and interview a Federal Prisoner (DOJ Memorandum "Use and Targeting of Federal Prisoners in Investigations," January 22, 2009).

C.3 (U) DEFINITIONS

(U) Federal Prisoner: For purposes within this section, a federal prisoner is one who is held in the custody of either the BOP or the USMS pursuant to an order of a court in connection with a criminal matter, regardless of where the person is housed.

(U) Use of a Federal Prisoner: Use of a federal prisoner means to employ a federal prisoner during an investigation in such a manner that the prisoner will interact with others who are not members of law enforcement (e.g., the prisoner will engage in a consensually monitored telephone call with a target) or the prisoner will be taken out of the custody of BOP or USMS

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(e.g., the prisoner is removed from the prison to assist the FBI in locating a hide out) or law enforcement will interact covertly with the prisoner (e.g., an undercover agent engages with the prisoner in the visiting room of the prison).

(U) Targeting a Federal Prisoner: “Targeting” a federal prisoner means that the federal prisoner is the target of the investigation and that investigative activity will directly interact with either the prisoner or the federal facility (e.g., as part of a money laundering investigation targeting a prisoner, the FBI wishes to engage in a consensually monitored conversation with the prisoner).

(U) Interview of a Federal Prisoner: Interview of a federal prisoner means to interact with a federal prisoner, overtly representing oneself as an FBI employee, in order to gather information.

C.3.1 (U) USE AND TARGETING A FEDERAL PRISONER

(U//FOUO) An FBI employee may request the use of or the targeting of a federal prisoner in an FBI Predicated Investigation by completing the DOJ “Request to Utilize or Target a BOP or USMS Prisoner for Investigative Purposes” form (herein the “DOJ form”) located on the CPO DIOG SharePoint site.

(U//FOUO) The FBI Employee must document the required information and approvals as specified below on the DOJ form. A copy of the form must be uploaded and serialized in the appropriate investigative file, after it has been approved by the field office SSA and submitted to the FBIHQ operational unit for consideration and coordination of approval by DOJ.

C.3.2 (U) INTERVIEW A FEDERAL PRISONER

(U//FOUO) An FBI employee may request to interview a federal prisoner in an FBI Assessment or Predicated Investigation by obtaining: the approval of the appropriate FBI official as specified below; and concurrence of the Warden/BOP or USMS, as appropriate, or an order of the court. The results of the interview should be documented with an EC or 302, as appropriate under the circumstances, and uploaded and serialized into the appropriate investigative file.

C.4 (U) APPROVAL REQUIREMENTS

C.4.1 (U) APPROVAL - USE AND TARGETING A FEDERAL PRISONER

(U//FOUO) The FBI employee must obtain the prior approval of the field office SSA and must document the required information using the required DOJ form to seek the approval of FBIHQ and DOJ for use or targeting a federal prisoner.

(U//FOUO) **DOJ Form:** The field office must submit the DOJ form to the appropriate FBIHQ operational unit for review and approval, as specified below. The FBIHQ operational unit will coordinate the review and approval process with DOJ, as specified below. The process is as follows:

A) (U//FOUO) The FBI employee must:

- 1) (U//FOUO) Obtain the approval of the field office SSA responsible for the Predicated Investigation;

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- 2) (U//FOUO) Obtain the written concurrence of the Warden/BOP/USMS, as appropriate;
- 3) (U//FOUO) Complete the DOJ “Request to Utilize or Target a BOP or USMS Prisoner for Investigative Purposes” form (“DOJ form”) located on the [DIOG SharePoint site](#);
- 4) (U//FOUO) Obtain a Sealed Court Order: If the request involves the temporary transfer of a federal prisoner from the custody of BOP or USMS to the FBI, then the AUSA must obtain a sealed court order authorizing the transfer of custody and must adhere to FBI guidelines for transporting a federal prisoner (see Section C.8 below);
- 5) (U//FOUO) Email the completed DOJ form to FBIHQ operational unit point-of-contact; and
- 6) (U//FOUO) If the request is approved by the Office of Enforcement Operations (OEO), DOJ the FBI employee must, within 15 days of completion of use or targeting of the prisoner, provide the FBIHQ operational unit with the information necessary to complete the final disposition Action Memorandum (See item C.5.1.B.4 below).

B) (U//FOUO) The FBIHQ operational unit must:

- 1) (U//FOUO) Review the DOJ form and obtain the approval of the appropriate operational Section Chief;
- 2) (U//FOUO) Forward by facsimile (fax) the DOJ form to OEO for consideration and approval (OEO fax # is (202) 514-5143);
- 3) (U//FOUO) Provide the field office timely notification of OEO’s decision whether to grant permission to use or target the prisoner; and
- 4) (U//FOUO) Within 30 days of completion of use or targeting of the prisoner, provide OEO with a final disposition Action Memorandum.

(U//FOUO) **Exigent Circumstances:** If there are exigent circumstances requiring an immediate response, OEO will accept oral requests for approval from the FBIHQ operational unit. Confirmation of the request and appropriate supporting information must, however, be submitted to OEO in writing as soon as possible after oral approval is obtained.

(U//FOUO) For questions or exigent circumstances, the field must contact the FBIHQ operational unit, who will be responsible for contacting the DOJ Chief of the Witness Security and Operations Unit at (202) 307-3314, OEO, or Deputy Chief of Special Operations, at (202) 514-3684.

(U//FOUO) *Note:* The DOJ Memorandum governing the Use and Targeting of Federal Prisoners is labeled “Sensitive Investigative Matter.” This is not a SIM as defined in DIOG Section 10. As such, this policy does not require CDC review and SAC approval.

C.4.2 (U) APPROVAL - INTERVIEW A FEDERAL PRISONER

(U//FOUO) The FBI employee must:

- A) (U//FOUO) Obtain the prior approval of the field office SSA to interview a federal prisoner in locations listed under Section C.6.B.1-3 below;
- B) (U//FOUO) Obtain the prior approval of the field office SSA and SAC to interview a federal prisoner in any location under Section C.6.B.4 below; and

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

C) (U//FOUO) Obtain the concurrence of the Warden/BOP/USMS, as appropriate.

C.5 (U) EXEMPTIONS TO DOJ APPROVAL REQUIREMENT

(U//FOUO) When all four of the following conditions are met, neither approval nor consultation with DOJ is required for a cooperating prisoner to engage in consensually monitored telephone calls, text messages, or computer communications once the prisoner has given consent. (This situation will typically occur when the prisoner is newly arrested and still in FBI or USMS custody):

- A) (U//FOUO) Cooperating prisoner is not in BOP custody or under BOP supervision (e.g., not in a BOP operated facility, BOP contract facility, BOP halfway house, or under BOP home detention/electronic monitoring);
- B) (U//FOUO) The prisoner will participate in consensual monitoring from one of the following locations:
 - 1) (U//FOUO) A detention facility not operated by BOP;
 - 2) (U//FOUO) A United States Attorney's Office (USAO);
 - 3) (U//FOUO) An office of an investigative agency; or
 - 4) (U//FOUO) A secure location under the control of the FBI;
- C) (U//FOUO) No follow-up activity by the prisoner that would require OEO approval is anticipated to occur as a result of the consensual monitoring; and
- D) (U//FOUO) The FBI employee supervising the consensual monitoring has complied with all FBI policies governing consensual monitoring.

(U) Note: Unless all four of the above conditions are met, the agent must have OEO approval to use a federal prisoner to engage in consensual monitoring.

(U//FOUO) Neither approval nor consultation with OEO is required for a cooperating prisoner to engage in a debriefing, polygraph, proffer, re-enactment at scene of a crime; or aiding in the location of a hide-out, etc., once the prisoner has given consent, if the prisoner will participate in such activity in one of the following locations:

- A) (U//FOUO) A detention facility, including one operated by the BPO or USMS;
- B) (U//FOUO) A United States Attorneys Office;
- C) (U//FOUO) An office of an investigative agency; or
- D) (U//FOUO) A secure location under the control of the FBI.

C.6 (U) EXTENSION REQUESTS

(U//FOUO) Agents may request extensions of the authority to use or target a prisoner in an FBI investigation by providing OEO with a written report containing the following:

- A) (U//FOUO) Up-to-date summary of use or targeting of the federal prisoner;
- B) (U//FOUO) Justification for continued use or targeting of the federal prisoner;
- C) (U//FOUO) Endorsement of AUSA;

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- D) (U//FOUO) Endorsement of the federal prisoner's counsel; and
- E) (U//FOUO) Warden/BOP/USMS concurrence.

C.7 (U) TRANSPORTATION OF FEDERAL PRISONER

(U//FOUO) If it is necessary to remove the federal prisoner from the detention facility in which he/she is housed as a part of the investigation, DOJ OEO policy mandates the following minimum standards for transfer of custody from BOP/USMS to the FBI for "Use or Targeting of a Federal Prisoner:"

- A) (U//FOUO) Prisoner must be restrained in leg shackles and handcuffs with a waist chain during transport;
- B) (U//FOUO) A trail vehicle must be used during transport;
- C) (U//FOUO) Prisoner must neither make nor receive any private visits or telephone calls;
- D) (U//FOUO) Prisoner must have no contact with the public, including in restaurants or restrooms;
- E) (U//FOUO) Prisoner must not consume alcoholic beverages;
- F) (U//FOUO) Prisoner must be given no advanced notice of his/her transfer from BOP/USMS to FBI;
- G) (U//FOUO) If overnight housing is necessary, prisoner must be kept in a USMS-approved detention facility; and
- H) (U//FOUO) The transportation must occur during daylight hours.

**APPENDIX D: (U) DEPARTMENT OF JUSTICE
MEMORANDUM ON COMMUNICATIONS WITH THE WHITE
HOUSE AND CONGRESS, DATED MAY 11, 2009**



Office of the Attorney General
Washington, D. C. 20530

May 11, 2009

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS
ALL UNITED STATES ATTORNEYS

FROM:

A handwritten signature, likely of the Attorney General, is written over the word "THE" in the "FROM:" line.

THE ATTORNEY GENERAL

SUBJECT:

Communications with the White House and Congress

The rule of law depends upon the evenhanded administration of justice. The legal judgments of the Department of Justice must be impartial and insulated from political influence. It is imperative that the Department's investigatory and prosecutorial powers be exercised free from partisan consideration. It is a fundamental duty of every employee of the Department to ensure that these principles are upheld in all of the Department's legal endeavors.

In order to promote the rule of law, therefore, this memorandum sets out guidelines to govern all communications between representatives of the Department, on the one hand, and representatives of the White House and Congress, on the other, and procedures intended to implement those guidelines. (The "White House," for the purposes of this Memorandum, means all components within the Executive Office of the President.) These guidelines have been developed in consultation with, and have the full support of, the Counsel to the President.

1. Pending or Contemplated Criminal or Civil Investigations and Cases

The Assistant Attorneys General, the United States Attorneys, and the heads of the investigative agencies in the Department have the primary responsibility to initiate and supervise investigations and cases. These officials, like their superiors and their subordinates, must be insulated from influences that should not affect decisions in particular criminal or civil cases. As the Supreme Court said long ago with respect to United States Attorneys, so it is true of all those who exercise the Department's investigatory and prosecutorial powers: they are representatives "not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done." *Berger v. United States*, 295 U.S. 78, 88 (1935).

a. In order to ensure the President's ability to perform his constitutional obligation to "take care that the laws be faithfully executed," the Justice Department will advise the White House concerning pending or contemplated criminal or civil investigations or cases when—but only when—it is important for the performance of the President's duties and appropriate from a law enforcement perspective.

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 2

b. Initial communications between the Department and the White House concerning pending or contemplated criminal investigations or cases will involve only the Attorney General or the Deputy Attorney General, from the side of the Department, and the Counsel to the President, the Principal Deputy Counsel to the President, the President or the Vice President, from the side of the White House. If the communications concern a pending or contemplated civil investigation or case, the Associate Attorney General may also be involved. If continuing contact between the Department and the White House on a particular matter is required, the officials who participated in the initial communication may designate subordinates from each side to carry on such contact. The designating officials must monitor subsequent contacts, and the designated subordinates must keep their superiors regularly informed of any such contacts. Communications about Justice Department personnel in reference to their handling of specific criminal or civil investigations or cases are expressly included within the requirements of this paragraph. This policy does not, however, prevent officials in the communications, public affairs, or press offices of the White House and the Department of Justice from communicating with each other to coordinate efforts.

c. In order to ensure that Congress may carry out its legitimate investigatory and oversight functions, the Department will respond as appropriate to inquiries from Congressional Committees consistent with policies, laws, regulations, or professional ethical obligations that may require confidentiality and consistent with the need to avoid publicity that may undermine a particular investigation or litigation. Outside the context of Congressional hearings or investigations, all inquiries from individual Senators and Members of Congress or their staffs concerning particular contemplated or pending criminal investigations or cases should be directed to the Attorney General or the Deputy Attorney General. In the case of particular civil investigations or cases, inquiries may also be directed to the Associate Attorney General.

d. These procedures are not intended to interfere with the normal communications between the Department and its client departments and agencies (including agencies within the Executive Office of the President when they are the Department's clients) and any meetings or communications necessary to the proper conduct of an investigation or litigation.

2. National Security Matters

It is critically important to have frequent and expeditious communications relating to national security matters, including counter-terrorism and counter-espionage issues. Therefore communications from (or to) the Deputy Counsel to the President for National Security Affairs, the staff of the National Security Council and the staff of the Homeland Security Council that relate to a national security matter are not subject to the limitations set out above. However, this exception for national security matters does not extend to pending adversary cases in litigation that may have national security implications. Communications related to such cases are subject to the guidelines for pending cases described above.

Memorandum for Head of Department Components
All United States Attorneys
Subject: Communications with the White House and Congress

Page 3

3. White House Requests for Legal Advice

All requests from the White House for formal legal opinions shall come from the President, the Counsel to the President, or one of the Deputy Counsels to the President, and shall be directed to the Attorney General and the Assistant Attorney General for the Office of Legal Counsel. The Assistant Attorney General for the Office of Legal Counsel shall report to the Attorney General and the Deputy Attorney General any communications that, in his or her view, constitute improper attempts to influence the Office of Legal Counsel's legal judgment.

4. Communications Involving the Solicitor General's Office.

Matters in which the Solicitor General's Office is involved often raise questions about which contact with the Office of the Counsel to the President is appropriate. Accordingly, the Attorney General and Deputy Attorney General may establish distinctive arrangements with the Office of the Counsel to govern such contacts.

5. Presidential Pardon Matters

The Office of the Pardon Attorney may communicate directly with the Counsel to the President and the Deputy Counsels to the President, concerning pardon matters. The Counsel to the President and the Deputy Counsels to the President may designate subordinates to carry on contact with the Office of the Pardon Attorney after the initial contact is made.

6. Personnel Decisions Concerning Positions in the Civil Service

All personnel decisions regarding career positions in the Department must be made without regard to the applicant's or occupant's partisan affiliation. Thus, while the Department regularly receives communications from the White House and from Senators, Members of Congress, and their staffs concerning political appointments, such communications regarding positions in the career service are not proper when they concern a job applicant's or a job holder's partisan affiliation. Efforts to influence personnel decisions concerning career positions on partisan grounds should be reported to the Deputy Attorney General.

7. Other Communications Not Relating to Pending Investigations or Criminal or Civil Cases

All communications between the Department and the White House or Congress that are limited to policy, legislation, budgeting, political appointments, public affairs, intergovernmental relations, or administrative matters that do not relate to a particular contemplated or pending investigation or case may be handled directly by the parties concerned. Such communications should take place with the knowledge of the Department's lead contact regarding the subject

Memorandum for Head of Department Components

Page 4

All United States Attorneys

Subject: Communications with the White House and Congress

under discussion. In the case of communications with Congress, the Office of the Deputy Attorney General and Office of the Assistant Attorney General for Legislative Affairs should be kept informed of all communications concerning legislation and the Office of the Associate Attorney General should be kept informed about important policy communications in its areas of responsibility.

As Attorney General Benjamin Civiletti noted in issuing a similar memorandum during the Carter Administration, these guidelines and procedures are not intended to wall off the Department from legitimate communication. We welcome criticism and advice. What these procedures are intended to do is route communications to the proper officials so they can be adequately reviewed and considered, free from either the reality or the appearance of improper influence.

Decisions to initiate investigations and enforcement actions are frequently discretionary. That discretion must be exercised to the extent humanly possible without regard to partisanship or the social, political, or interest group position of either the individuals involved in the particular cases or those who may seek to intervene against them or on their behalf.

This memorandum supersedes the memorandum issued by Attorney General Mukasey on December 19, 2007, titled *Communications with the White House*.

**APPENDIX E: (U//FOUO) ATTORNEY GENERAL
MEMORANDUM – REVISED POLICY ON THE USE OR
DISCLOSURE OF FISA INFORMATION, DATED JANUARY 10,
2008**



U.S. Department of Justice

National Security Division

Office of the Assistant Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All United States Attorneys
All National Security Division Attorneys
All Anti-Terrorism Coordinators

CC: Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Kenneth L. Wainstein *KLW*
Assistant Attorney General for National Security

SUBJECT: Revised FISA Use Policy as Approved by the Attorney General

We are pleased to provide the Department of Justice's revised policy on the use or disclosure of information obtained or derived from collections under the Foreign Intelligence Surveillance Act of 1978 (FISA), as approved by the Attorney General today. Also attached is a form for use with respect to notifications that are required under Section I of the revised policy.

This revised policy includes significant changes from current practice that will streamline the process for using FISA information in certain basic investigative processes, while still ensuring that important intelligence and law enforcement interests are protected.

You will note that the revised policy authorizes the use or disclosure of FISA information, under the specific circumstances described in the policy, with notification to NSD and after consultation with the FBI (or other Intelligence Community agencies) for the following investigative processes:

- grand jury subpoenas for third-party documents to corporations, institutions, and other providers of commercial services (where the entities are neither the subjects nor targets of the investigation and from which there is no known substantial risk of improper disclosure);

FOR OFFICIAL USE ONLY

- noncompulsory requests for third-party documents to corporations, institutions, and other providers of commercial services (where the entities are neither the subjects nor targets of the investigation and from which there is no known substantial risk of improper disclosure);
- custodian of records testimony before the grand jury for such subpoenaed parties; and
- criminal pen register and trap and trace device applications (except where the FISA information used in the PR/TT application goes beyond the relevant identifier(s)).

As described in the revised policy, the Department continues to require prior authorization from the Assistant Attorney General for National Security (AAG/NSD) for the use or disclosure of FISA information in order to file criminal charges or in post-charge criminal proceedings, as well as in connection with certain investigative processes (*e.g.*, criminal search warrants under Rule 41 of the Federal Rules of Criminal Procedure). The revised policy also requires the prior authorization of the AAG/NSD or his designee for the use or disclosure of FISA information in non-criminal proceedings.

The revised policy was drafted by a Justice Department working group that included representatives from the Attorney General's Advisory Committee of United States Attorneys (AGAC), National Security Division (NSD), Federal Bureau of Investigation (FBI), and Office of Legal Policy (OLP). The working group also consulted with the Office of the Director of National Intelligence (ODNI) in the course of the development of this policy.

The revised policy requires that it be reviewed one year from its effective date and requires NSD to issue guidance on what constitutes information "derived from" FISA collections by March 31, 2008.

As noted in the policy, prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

FOR OFFICIAL USE ONLY



U.S. Department of Justice


Office of the Attorney General

Washington, D.C. 20530

January 10, 2008

TO: All Federal Prosecutors

CC: Assistant Attorney General, National Security Division
Assistant Attorney General, Criminal Division
Assistant Attorney General, Civil Division
Director, Federal Bureau of Investigation

FROM: Michael B. Mukasey 
Attorney General

SUBJECT: Revised Policy on the Use or Disclosure of FISA Information

As a general matter, it is the policy of the Department of Justice to use all lawful processes in the investigation and prosecution of cases involving terrorism, intelligence, and national security, and to undertake all efforts necessary to protect the American people from the threat posed by foreign powers and their agents, while also exercising due regard for the protection of intelligence sources, methods, and collections, and the privacy and civil liberties of United States persons.

There are important purposes to be served by consultation and coordination with respect to the use or disclosure of FISA information¹ in investigations, criminal prosecutions, and other proceedings. First, because FISA information is almost always classified, the use or disclosure of such information will normally require declassification by the originating agency in accordance with the originating agency's policies and procedures. Second, the use of such information could directly or indirectly compromise intelligence sources, methods, or collections, or disclose the existence or nature of or otherwise compromise an investigation. Third, FISA requires the Government to notify the court and an "aggrieved person" of its intent

¹ The term "FISA information," as used in this policy, means any information acquired, obtained, or derived from collection authorized pursuant to FISA. Whether specific information qualifies as "derived from" FISA collection may be a fact-bound question that depends, at least in part, on the attenuation of the information to be used from the original FISA acquired or obtained information and whether the information was also obtained from an independent source, as well as other factors. Where such a question arises, the application of this policy should be discussed among the USAO, FBI, and NSD, and if consensus is not reached, a determination will be made by the Assistant Attorney General for National Security. Separate guidance regarding what constitutes information "derived from" FISA collection will be issued by the National Security Division no later than March 31, 2008.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

to use or disclose any FISA information before it is used against such person in a broad range of proceedings. Fourth, the Government is required to ensure that complete and accurate filings are made with the Foreign Intelligence Surveillance Court (FISC), and that the Government complies with all of FISA's statutory requirements. Fifth, it is important to ensure that litigation risks, if any, are properly assessed. Finally, in certain cases, it may be appropriate to make disclosures to a United States District Court regarding classified facts before legal process is obtained.

Given these purposes, it is essential that coordination take place in connection with the use or disclosure of FISA information. Such coordination should be streamlined in order to promote efficient, nimble, and useful investigative activities. The risk of compromising the purposes described above varies depending on the stage of the investigation, criminal prosecution, or other proceeding. As a general matter, the risks are comparatively smaller during an investigation than during a criminal trial or other proceeding. The use or disclosure of FISA information in non-criminal proceedings may present varying levels of risk. Because FISA information is almost always classified, federal prosecutors should consider alternative approaches for taking action.

Prosecutors are encouraged to contact the National Security Division at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.

The following policy is therefore adopted and supersedes any existing Attorney General policies with respect to the use and disclosure of FISA information to the extent that they are inconsistent with this policy:

- (a) the Assistant Attorney General for National Security may act as the Attorney General, as provided for under FISA, *see* 50 U.S.C. § 1801(g), for the purpose of authorizing the use or disclosure of FISA information pursuant to this policy;² and
- (b) federal prosecutors and all others who may seek to use or disclose FISA information in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, in coordination with NSD and FBI, are authorized to do so pursuant to the terms of this policy, shall coordinate with NSD in regard to any litigation that results from the use or disclosure of FISA information, and shall comply with the following procedures in matters that involve the use or disclosure of FISA information.³

² Such authorization may also be provided by the Attorney General, Acting Attorney General, and the Deputy Attorney General. *See* 50 U.S.C. § 1801(g).

³ Nothing in this policy is intended to supersede or replace existing policies for prosecutors regarding notification, consultation, and approval for certain investigative and prosecutive steps, including consultation with other districts where related matters may be under investigation. For example, the United States Attorneys' Manual sets forth when a prosecutor must obtain prior approval for various court actions in national security prosecutions. *See, e.g.,* United States Attorneys' Manual (USAM) §§ 9-2.131 ("Matters Assumed by Criminal Division or Higher

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

I. Use or Disclosure of FISA Information Requiring Consultation with FBI or other Intelligence Community Agencies and Notification to NSD

- A. Certain investigative processes present only moderate risks. As a result, where FISA information is used or disclosed in connection with the processes described below, consultation with FBI (or other Intelligence Community agencies, as appropriate)⁴ and notice to NSD is required:
1. Non-compulsory requests for third-party documents to corporations, institutions, and other providers of commercial services, including but not limited to communications service providers and financial institutions, that are neither the subject nor target of the national security investigation and from which there is no known substantial risk of improper disclosure.
 2. Grand jury subpoenas for third-party documents to corporations, institutions, and other providers of commercial services, including but not limited to communications service providers and financial institutions, that are neither the subject nor target of the national security investigation and from which there is no known substantial risk of improper disclosure.
 3. Testimony before the grand jury by the custodian of records for such a subpoenaed party.
 4. Pen registers or trap and trace devices under Title 18, Chapter 206, United States Code.⁵
- B. Where FISA information is used or disclosed in connection with the processes described above, the following notification process shall be followed:
1. The federal prosecutor shall provide written notification (see attached draft notification form), in a secure format, to NSD.

Authority"); 9-2.136 ("Investigative and Prosecutive Policy for International Terrorism Matters"); 9-2.155 ("Sensitive Matters"); 9-2.400 ("Prior Approvals Chart").

⁴ For the purposes of this document, the term "Intelligence Community agencies" refers to the appropriate agencies within the Intelligence Community, including the Office of the Director of National Intelligence. Consultation with Intelligence Community agencies other than the FBI is typically appropriate when the sources, methods, or collections involve Intelligence Community agencies other than the FBI. Prosecutors are encouraged to contact the National Security Division, as needed, to assist with the consultation process with the FBI or other Intelligence Community agencies.

⁵ Some courts require a significant measure of information with respect to applications for pen register or trap and trace devices. To the extent that applications in such districts require the disclosure of additional FISA information beyond the disclosure of the target phone number(s) or other identifiers relevant to the pen register or trap and trace device, advance authorization as provided for in Section II of this policy is required prior to such applications being made to the court.

FOR OFFICIAL USE ONLY

2. As provided on the attached draft notification form, the federal prosecutor must indicate that he or she has consulted with the FBI's Classified Litigation Support Unit (or other Intelligence Community agencies, as appropriate) with respect to the use or disclosure of the FISA information.
 3. Such notification must occur as early as possible—and where feasible, either before or simultaneous to the use of the processes described above—to ensure that NSD complies with potential obligations to notify the Foreign Intelligence Surveillance Court.
- C. Where consultations with the FBI (or other Intelligence Community agencies, as appropriate) demonstrate that the use of such processes is reasonably likely to result in the compromise of an investigation, or the FISA information was obtained or derived from particularly sensitive sources, methods, or collections,⁶ further consultation that includes NSD (working with Intelligence Community agencies, as appropriate) shall take place prior to the use of such processes.
1. Where such further consultation takes place because of particularly sensitive sources, methods, or collections, NSD shall provide notice of such consultation to ODNI.
- D. This section does not permit the use or disclosure of FISA information obtained from such processes in order to file criminal charges by complaint, information, or indictment, or in post-charge criminal proceedings.⁷ Federal prosecutors must seek specific, separate use authority from the Assistant Attorney General for National Security prior to initiating any criminal proceedings.
- II. Use or Disclosure of FISA Information Requiring the Advance Authorization of the Assistant Attorney General for National Security
- A. The advance authorization of the Assistant Attorney General for National Security is required where FISA information is used or disclosed in order to file criminal charges by complaint, information, or indictment, or in post-charge criminal proceedings, and before FISA information may be used or disclosed in connection with the processes discussed below.

⁶ The phrase "particularly sensitive sources, methods, or collections," as used herein, refers to those sources, methods, or collections that raise significant concerns to the FBI or other Intelligence Community agencies, as appropriate, beyond those generally present in all activities conducted under FISA.

⁷ This statement refers to FISA information obtained from processes in Section I.A of this policy that is, or that the prosecution reasonably expects may be, used as evidence or disclosed in any manner in a complaint, information, or indictment, or in post-charge criminal proceedings.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

1. *Investigative Processes Requiring Advance Authorization*
 - a. Certain investigative processes present potentially higher risks. As a result, authorization of the Assistant Attorney General for National Security is required before FISA information is used or disclosed in connection with the processes described below:
 - i. grand jury subpoenas, other than the non-testimonial third-party grand jury subpoenas of the type described above;
 - ii. interception of communications under Title 18, Chapter 119, United States Code;
 - iii. accessing stored wire and electronic communications and transactional records under Title 18, Chapter 121, United States Code;
 - iv. search warrants under Rule 41 of the Federal Rules of Criminal Procedure;
 - v. material witness warrants under 18 U.S.C. § 3144;
 - vi. witness testimony before a grand jury, except as described above; or
 - vii. any investigative tool other than those described in this document, whose use in a particular investigation, in the view of the federal prosecutor, NSD, or the FBI (or other Intelligence Community agencies, as appropriate), would be reasonably likely to result in an compromise of the investigation, or in the compromise of particularly sensitive sources, methods, or collections.
2. *Criminal Indictments and Post-Indictment Proceedings*
 - a. The use or disclosure of FISA information to file criminal charges by complaint, information, or indictment, or in post-charge criminal proceedings presents significant risks. As a result, the advance authorization of the Assistant Attorney General for National Security is required before such use or disclosure.
 - b. This advance authorization requirement applies to FISA information that is, or that the prosecution reasonably expects may be, used as evidence or disclosed in any manner in a complaint, information, or indictment, or in post-charge criminal proceedings.

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

3. Among the factors that will be considered with respect to granting use authority are: (a) the importance of the information in a proceeding to disrupt a terrorist related operation, incapacitate the subjects, or create incentives for the subjects to provide intelligence; (b) the protection of intelligence sources, methods, and collections; (c) the impact on other proceedings or investigations; (d) FISA's statutory requirements, including the requirement that notice be given to a person who would be considered an "aggrieved person" under the statute and against whom FISA information is being used or disclosed; (e) the Government's compliance with the applicable minimization procedures authorized by the FISC; and (f) the litigation risks, including discovery issues, if any.
4. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, federal prosecutors should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require declassification and consideration of issues related to sources, methods, and collections by the FBI and other Intelligence Community agencies, federal prosecutors should work with the FBI and other Intelligence Community agencies prior to seeking such advance authorization, as appropriate.
 - a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
 - b. Where advance authorization involving particularly sensitive sources, methods, or collections is requested, NSD shall provide notice of such request to ODNI.

III. Use or Disclosure of FISA Information In Non-Criminal Proceedings

- A. The use or disclosure of FISA information in non-criminal proceedings may present varying levels of risk. Therefore, authorization of the Assistant Attorney General for National Security or his designee is required before such use or disclosure.
 1. For the purpose of this policy, the phrase "non-criminal proceeding" refers to any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States that does not involve the potential imposition of a criminal sanction. Cf. 50 U.S.C. § 1806(c); 50 U.S.C. § 1825(d).

FOR OFFICIAL USE ONLY

2. Among the factors that will be considered with respect to granting use authority are: (a) the importance of the information in a proceeding to disrupt a terrorist related operation, incapacitate the subjects, or create incentives for the subjects to provide intelligence; (b) the protection of intelligence sources, methods, and collections; (c) the impact on other proceedings or investigations; (d) FISA's statutory requirements, including the requirement that notice be given to a person who would be considered an "aggrieved person" under the statute and against whom FISA information is being used or disclosed; (e) the Government's compliance with the applicable minimization procedures authorized by the FISC; and (f) the litigation risks, including discovery issues, if any.
 3. Because the process of obtaining advance authorization will require NSD to coordinate with Intelligence Community agencies, the attorney for the government should seek such advance authorization at the earliest juncture possible. In addition, because the use of such information will normally require declassification and consideration of issues related to sources, methods, and collections by the FBI and other Intelligence Community agencies, the attorney for the government should work with the FBI and other Intelligence Community agencies prior to seeking such advance authorization, as appropriate.
 - a. Prosecutors are encouraged to contact NSD at any time in order to obtain guidance regarding this policy and to expedite resolution of any issues.
 - b. Where advance authorization involving particularly sensitive sources, methods, or collections is requested, NSD shall provide notice of such request to ODNI.
- This policy shall be reviewed one year from its effective date to evaluate its effectiveness.

FOR OFFICIAL USE ONLY

Classification:

NOTIFICATION OF USE OR DISCLOSURE OF FISA INFORMATION FORM

This form is to be used when notifying the National Security Division regarding the use or disclosure of information obtained or derived from collection authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, in accordance with Section I of the Attorney General's Revised Policy on the Use or Disclosure of FISA Information (relating to the use or disclosure of FISA information with respect to certain investigative processes). Federal prosecutors may notify the National Security Division by sending the completed form to: fisa.use@nsd.usdoj.sgov.gov (SECRET or below information only) or by secure faxing the form to 202-514-9262. **A PDF-fillable version of this form is available on SIPRnet in USAO district folders on the "G:" drive of JCON-S under the sub-folder, CTS Resource Library.**

In addition, federal prosecutors are encouraged to contact at any time the NSD Office of Intelligence Litigation Section at (202) 514-5600, the Counterterrorism Section through the designated trial attorney or the Regional ATAC Coordinator at (202) 514-0849, or the Counterespionage Section through the designated trial attorney or at (202) 514-1187. NSD duty attorneys can be reached after business hours through the DOJ Command Center at (202) 514-5000.

Blank versions of this form are unclassified. **Please add classification markings to the form according to the classification of the information you provide.**

1. Name of FISA target(s): _____
2. FISA Court docket numbers for the orders authorizing the collection that produced the information sought to be used or disclosed (list all):

3. Nature of activity for which the FISA information will be used or disclosed (e.g., investigative process (please specify type), criminal proceeding, non-criminal proceeding): _____
4. Title and court of proceeding (if applicable):

5. Target(s) and subject(s) of the investigation (list all):

6. USAO point of contact:
Name: _____
Telephone and Fax (unclassified and secure): _____
E-mail address (unclassified and classified): _____

Classification:

Classification:

7. NSD point(s) of contact (list all):

Name(s): _____

Telephone and Fax (unclassified and secure): _____

E-mail address (unclassified and classified): _____

8. Has consultation with FBI's Classified Litigation Support Unit, National Security Law Branch, (202) 324-3951 (or other Intelligence Community agencies, as appropriate) taken place? _____

9. Please identify the point of contact for FBI (or other Intelligence Community agencies, as appropriate):

Name: _____

Telephone and Fax (unclassified and secure): _____

E-mail address (unclassified and classified): _____

10. Please provide a brief description of the nature of the investigation and also describe how FISA information will be used or disclosed (e.g., grand jury subpoena for telephone subscriber records and credit card records):

Date: _____

Submitted By _____

Title _____

Telephone Number _____

Classification:

APPENDIX F: (U) USE OF FORCE POLICY

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

B) (U) Instructional Outline and Use of Force Scenarios.

F.1 (U) USE OF LESS-THAN-LETHAL DEVICES

(U) Deputy Attorney General's Memorandum on Use of Less-than-Lethal Devices dated 4/21/2011.



The Deputy Attorney General

Washington, D.C. 20530

May 16, 2011

MEMORANDUM FOR

Robert S. Mueller III
Director
Federal Bureau of Investigation

Michele M. Leonhart
Administrator
Drug Enforcement Administration

Kenneth E. Melson
Acting Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

Stacia A. Hylton
Director
United States Marshals Service

Thomas R. Kane
Acting Director
Federal Bureau of Prisons

FROM:

James M. Cole 
Deputy Attorney General

SUBJECT:

Policy on the Use of Less-Than-Lethal Devices

Attached is the Department's Policy on the Use of Less-Than-Lethal Devices, approved by the Attorney General on April 21, 2011. Please ensure that the policy is distributed to every affected employee within your component.

Attachment

DEPARTMENT OF JUSTICE POLICY STATEMENT
ON THE USE OF LESS-THAN-LETHAL DEVICES

- I. Department of Justice (DOJ) law enforcement officers (officers) are authorized to use less-than-lethal devices only as consistent with this policy statement.
- II. Pursuant to this policy statement, less-than-lethal devices:
 - A. Are synonymous with "less lethal," "non-lethal," "non-deadly," and other terms referring to devices used in situations covered by this policy statement; and
 - B. Include, but are not limited to:
 - 1. Impact Devices (e.g., batons, bean bag projectiles, baton launcher, rubber projectiles, stingballs);
 - 2. Chemical Agents (e.g., tear gas, pepper spray, pepperballs); and
 - 3. Conducted Energy Devices (e.g., electronic immobilization, control, and restraint devices).
- III. DOJ officers are authorized to use less-than-lethal devices only in those situations where reasonable force, based on the totality of the circumstances at the time of the incident, is necessary to effectuate an arrest, obtain lawful compliance from a subject, or protect any person from physical harm. Use of less-than-lethal devices must cease when it is no longer necessary to achieve the law enforcement objective.
- IV. DOJ officers are authorized to use only those less-than-lethal devices authorized by their component and that they are trained to use, absent exigent circumstances.
- V. DOJ officers are not authorized to use less-than-lethal devices if voice commands or physical control achieve the law enforcement objective. DOJ officers are prohibited from using less-than-lethal devices to punish, harass, or abuse any person.
- VI. Less-than-lethal devices are used with a reasonable expectation that death or serious bodily injury will not

result. They are, however, recognized as having the potential to cause death or serious bodily injury, and DOJ officers may use less-than-lethal devices as deadly weapons only when authorized under the DOJ Policy Statement on the Use of Deadly Force.

- VII. DOJ officers must make necessary medical assistance available to subjects of less-than-lethal device use as soon as practicable.
- VIII. DOJ components must establish rules and procedures implementing this policy statement. Each component will ensure that state/local officers participating in joint task force operations are aware of and adhere to the policy and its limits on DOJ officers.
- IX. DOJ components must establish training programs and procedures for using less-than-lethal devices that are consistent with this policy statement and federal law.
- X. DOJ components must individually establish procedures for documenting, reporting, reviewing, and investigating (as warranted), all incidents involving the use of less-than-lethal devices.
- XI. This policy statement is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

F.2 (U) USE OF DEADLY FORCE

(U) Deadly Force Policy, dated 7/1/2004.

POLICY STATEMENT USE OF DEADLY FORCE

GENERAL PRINCIPLES

1. Law enforcement officers and correctional officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.
 - A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
 - B. Firearms may not be fired solely to disable moving vehicles.
 - C. If feasible and if to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.
 - D. Warning shots are not permitted outside of the prison context.
 - E. Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by this policy.

CUSTODIAL SITUATIONS

- II. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons
 - A. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or
 - B. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.
- III. If the subject is in a non-secure facility deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or another person.

- IV. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.
- V. After an escape from a facility or vehicle and its immediate environs has been effected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.
- VI. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended Subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.
- VII. In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons: (A) If reasonably necessary to deter or prevent the subject from escaping from a secure facility or (B) if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

APPLICATION OF THE POLICY

VIII. This Policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

♦♦

F.3 (U) TRAINING

A) (U) Deadly Force Policy Training Material, dated 7/29/2004.

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/29/2004

To: All Divisions

Attn: AD
ADIC
SAC
CDC
PFI
FBIHQ, Manuals Desk
FBIHQ, Manuals Desk

From: General Counsel

Legal Instruction Unit

Contact: Lisa A. Baker, 703/632-3137

Approved By: Caproni Valerie E
Kelley Patrick W

Drafted By: Baker Lisa A

Case ID #: 66F-HQ-1312253
66F-HQ-C1384970
66F-HQ-C1384970

Title: REVISIONS TO THE DEPARTMENT OF
JUSTICE DEADLY FORCE POLICY -
DISSEMINATION OF TRAINING MATERIALS

Synopsis: This Electronic Communication (EC) provides recipients with training materials incorporating the revisions approved on July 1, 2004 to the Department of Justice (DOJ) Deadly Force Policy.

Reference: 66F-HQ-1312253 Serial 8

Enclosure(s): One copy of an instructional outline and one copy of use of force scenarios provided to all recipients for training purposes.

Details: As discussed in the referenced EC, dated 7/7/2004, on July 1, 2004, the Attorney General approved a revised Policy Statement on the use of Deadly Force. In order to assist Field Offices in providing training and guidance on the practical application of the Deadly Force Policy in light of the revised language, the Legal Instruction Unit (LIU), Office of the General Counsel, revised training materials used with the prior Policy Statement to reflect the changes approved by the Attorney General.

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

The training materials consist of an Instructional Outline and a set of 13 factual scenarios with a discussion of the use of force within the scenario and whether its use violates the policy. This material is similar to what was used for instructional purposes since 12/1/1995. The revised material reflects what was noted in the EC, that the revised policy does not expand or contract the current justification for the use of deadly force. Nonetheless, revisions to the training materials were necessary in order to describe the application of deadly force consistent with the new more succinct policy statement.

The revisions to the training materials primarily relate to the elimination of the "safe alternative" language as a function of the "necessity" for use of deadly force and elimination of language addressing the use of deadly force to prevent the escape of a fleeing felon. For a more detailed discussion of the nature of the revised Policy Statement and the basis for these revisions, refer to the referenced EC.

To: All Divisions From: General Counsel
Re: 66F-HQ-1312253, 07/29/2004

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

It is requested that this communication be distributed
to all appropriate personnel.

♦♦

DEADLY FORCE POLICY
TRAINING MATERIAL - 7/29/2004

DEPARTMENT OF JUSTICE DEADLY FORCE POLICY¹

Law enforcement officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.

- A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
- B. Firearms may not be fired solely to disable moving vehicles.
- C. If feasible and to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.
- D. Warning shots are not permitted²
- E. Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by this policy.

This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

¹Department of Justice Policy Statement Use of Deadly Force (07/01/2004) in pertinent part (Language relating to Custodial Situations has been intentionally omitted pursuant to FBI policy. See, 66F-HQ-1312253, EC from the Director's Office to All Divisions, titled "REVISIONS TO THE DEPARTMENT OF JUSTICE DEADLY FORCE POLICY", dated 07/07/2004).

²Not included in the above description is the policy relating to the use of deadly force to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons. Because Agents will seldom find themselves in a position to apply the custodial aspect of the policy, the FBI will adhere to the policy decision set forth in the Airtel from the Director to All Field Offices, titled "Deadly Force Policy Matters," dated 1/5/95, which states "A policy decision has been made that except in cases of prison unrest which would principally involve HRT and/or SWAT, FBI Agents should adhere to the policy and training principles governing the use of deadly force in non-custodial situations.

F.3 (U) TRAINING

B) (U) Instructional Outline and Use of Force Scenarios.

07/29/2004

INSTRUCTIONAL OUTLINE

I. INTRODUCTION

The following general principles shall guide the interpretation and application of this policy:

- A. This policy shall not be construed to require Agents to assume unreasonable risks to themselves.
- B. The reasonableness of an Agent's decision to use deadly force must be viewed from the perspective of the Agent on the scene without the benefit of 20/20 hindsight.
- C. Allowance must be made for the fact that Agents are often forced to make split-second decisions in circumstances that are tense, uncertain, and rapidly evolving.

II. DEFINITIONS

- A. "DEADLY FORCE": Is force that is reasonably likely to cause death or serious physical injury.
- B. "REASONABLE BELIEF": Is synonymous with "Probable Cause". It is determined by a totality of the facts and circumstances known to Agents at the time, and the logical inferences that may be drawn from them.
- C. "NECESSARY": The necessity to use deadly force based on the existence of a reasonable belief that the person against whom such force is used poses an imminent danger of death or serious physical injury to the Agent or other persons.
- D. "IMMINENT DANGER": "Imminent" does not mean "immediate" or "instantaneous", but that an action is pending. Thus, a subject may pose an imminent danger even if he is not at that very moment pointing a weapon at the Agent. For example, imminent danger may exist if Agents have probable cause to believe any of the following:

1. The subject possess a weapon, or is attempting to gain access to a weapon, under circumstances indicating an intention to use it against the Agents or others; or,
2. The subject is armed and running to gain the tactical advantage of cover; or,
3. A subject with the capability of inflicting death or serious physical injury--or otherwise incapacitating agents--without a deadly weapon, is demonstrating an intention to do so; or,
4. The subject is attempting to escape from the vicinity of a violent confrontation in which the suspect inflicted or attempted the infliction of death or serious physical injury.

III APPLICATION OF DEADLY FORCE

In assessing the necessity to use deadly force, the following practical considerations are relevant to its proper application:

A. Inherent Limitation on Abilities to Assess the Threat and Respond.

1. Limited Time (Action v. Reaction) - there will always be an interval of time between a subject's action and an Agent's ability to perceive that action, to assess its nature, and to formulate and initiate an appropriate response. The inherent disadvantage posed by the action/reaction factor places a significant constraint on the time frame within which Agents must perceive, assess and react to a threat.
2. Limited Means (Wound Ballistics) - When the decision is made to use deadly force, Agents have *no guaranteed means of instantaneously stopping the threat*. The human body can sustain grievous - even ultimately fatal - injury and continue to function for a period of time (from several seconds to several minutes) depending on the location, number, and severity of the wounds. The lack of a reliable means of instantaneously stopping the threat, may extend the time that imminent danger can persist. This factor further constrains the time frame within which Agents must respond to a perceived threat.

B. Achieving Intended Purpose.

1. Deadly force may only be applied for the intended purpose of bringing an imminent danger of death or serious physical injury to a timely halt either through the surrender of the subject or through physiological incapacitation.

If the subject does not surrender, the only reliable means of achieving that goal is to cause physiological incapacitation of the subject(s) as quickly as possible. Attempts to do anything else - such as shooting to cause minor injury - are unrealistic and can risk exposing Agents or others to continued danger of death or serious physical injury.

2. When the circumstances justify the use of deadly force, Agents should continue its application until the imminent danger is ended through the surrender or physiological incapacitation of the subject(s).

C. Consideration of Risk to Other Parties.

Even when deadly force is permissible, Agents should assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

SCENARIO #1: ARMED, RESISTING

Agents approach a residence at night to arrest a bank robbery subject. The robbery occurred six weeks earlier, and the robber threatened bank personnel with a handgun. Agents go to the front door of the house while others cover from their assigned positions. One Agent gains a view of the lighted interior of the house through an uncurtained window. When the Agents at the front door knock and announce their identity and purpose, the Agent watching through the window sees a man matching the description of the subject pick up a rifle and approach the door with gun in hand. The Agent fires through the glass, striking the subject in the back and side.

DISCUSSION: The use of deadly force is permissible

Deadly force is necessary to eliminate the imminent danger to the other Agents. The subject armed himself with a deadly weapon after the Agents had announced their identity and purpose; it is reasonable to believe that he has armed himself in preparation for violent resistance. Verbal warnings are not feasible due to the imminent nature of the threat.

SCENARIO #2: ARMED, RESISTING

An undercover Agent purchases three kilos of cocaine from two subjects seated in an automobile in a deserted parking lot at about 3:00 A.M. Through a pre-arranged signal, the Agent alerts a nearby team of Agents to move in and arrest the subjects. As the arrest team approaches on foot and the Agents on the team identify themselves as law enforcement officers and demand that the subject's place their hands where they can see them, the subjects' car suddenly veers toward them with the apparent intent to strike them. The Agents open fire, striking the driver.

DISCUSSION: The use of deadly force is permissible

It is reasonable for the Agents to believe the subjects pose an imminent danger to the Agents by using the vehicle as a deadly weapon, rather than just as a means of escape. Unlike the situation where a subject is using a vehicle merely to escape, the vehicle in this scenario is being used as a weapon to attack the Agents. A vehicle used in this manner poses no less an imminent danger than a firearm or other weapon, and deadly force is permissible to protect the Agents and others in the vicinity. Furthermore, Agents would not be required to permit the subjects to escape from the vicinity of a violent confrontation in which they have just attempted to inflict death or serious physical injury on the Agents. Verbal warnings were given before the Agents opened fire, but were ignored. Obviously, Agents confronted with a threat from an approaching vehicle should take evasive action to avoid getting killed or seriously injured; but the same may be said when Agents are confronted by subjects with knives or firearms. Because the vehicle was being used to attempt to kill or injure the Agents, it is not necessary that there be another threat or danger before the use of deadly force is permissible. Attempting to counter the danger by disabling the vehicle is impractical and contrary to policy. Thus, when deadly force is deemed necessary, it must be directed at the person or persons who pose a danger. As in all other instances where the use of deadly force is at issue, consideration must be given to whether its use creates a danger to third parties that outweighs its benefits.

SCENARIO #3: NON-DANGEROUS, ESCAPING

Agents possess an arrest warrant for a man who is wanted for Bank Fraud & Embezzlement. As they approach his residence to make the arrest, they observe a man matching the subject's description standing on the front porch. When the Agents are within about 20 yards of the residence, the man looks in their direction and immediately jumps from the porch and runs down the sidewalk away from them. One of the Agents shouts, "FBI! Stop!" When the man ignores that command, the Agent shouts a second time, "FBI! Stop or I'll shoot!" The man continues running, increasing the distance between himself and the pursuing Agents. Realizing that they are not going to be able to overtake the him, the Agent fires a shot, striking the man in the back.

DISCUSSION: The use of deadly force violates policy

Deadly force may only be used when necessary, that is when Agents have a reasonable belief that the subject of the force poses an imminent danger of death or serious physical injury. In this scenario, it is not reasonable to believe that the subject poses an imminent danger to the Agents or to others. If the Agents are unable to seize the subject without resort to deadly force, the subject will avoid arrest for the time being.

SCENARIO #4: ARMED, ESCAPING

Agents approach a residence during the day to arrest a bank robbery subject who threatened bank personnel with a handgun during the robbery. Before the Agents are able to fully establish a perimeter, a person matching the description of the subject bursts from the back door of the residence with what appears to be a pistol in his hand and runs through the back yard towards adjacent homes. Agents shout, "FBI! Stop! Or we'll shoot!" Ignoring the commands, the subject continues to run. An Agent fires a shot from a distance of about 15 yards, striking the subject in the back.

DISCUSSION: The use of deadly force is permissible

The Agent has probable cause (reasonable belief) that the subject, who has armed himself with a firearm, has done so to resist arrest and poses an imminent danger to the Agents in the immediate vicinity. The subject ignored commands to stop. As long as the fleeing armed subject remains within gunshot range of the Agents, he has the ability to turn and fire upon them before they can effectively respond by taking cover or returning fire. Attempting to pursue an armed subject increases that danger. In addition, the subject poses an imminent danger to those Agents who are trying to form the perimeter and whom the subject is likely to encounter as he continues his flight.

In deciding whether to use deadly force in this scenario, Agents should also consider that the subject is fleeing in a neighborhood setting. Accordingly, Agents should assess whether its use creates a danger to third parties that outweighs the likely benefits of its use.

SCENARIO #5: ARMED, RESISTING

An undercover Agent, posing as a fence for stolen property, is purchasing explosives and ammunition believed to be stolen from a military base. The subject arrives at the rendezvous, shows the merchandise and asks to see the money. When the Agent shows the money, the subject suddenly pulls a handgun and says, "I'll take that." The Agent hands over the money, and raises his hands. As the subject backs toward his truck, backup Agents emerge from their places of concealment, identify themselves as FBI Agents, and order the subject to drop the gun. The subject quickly glances in the direction of the Agents, but continues to point the gun in the direction of the undercover Agent. The backup Agents fire.

DISCUSSION: The use of deadly force is permissible

There is a reasonable belief that the armed subject poses an imminent danger to the undercover Agent from the moment the subject draws his handgun. Immediate action is necessary to protect the undercover Agent. Given the immediacy of the threat, the use of deadly force would be permissible when the subject drew his weapon.

SCENARIO #6: UNARMED, RESISTING

Agents attempt to execute an arrest warrant on a Fraud by Wire subject in the break room of a manufacturing plant where he works. The subject, a man of average size with no history of violence, is wearing pants and a shirt, and there is no indication that he is armed. When the Agents identify themselves and approach the subject, he suddenly exercises a precise karate kick, striking one of them in the groin and temporarily disabling him. One of the Agents backs away, draws his handgun, and orders the subject to surrender. The subject ignores the commands, adopts a martial arts fighting stance, and moves toward the Agent. The Agent fires.

DISCUSSION: The use of deadly force is permissible

It is reasonable for the Agents to believe that the subject is posing an imminent danger of death or serious physical injury to the Agents by his attack. The subject is not only capable of inflicting death or serious physical injury through his martial arts skills, but he also has the capacity to render the Agents incapable of defending themselves. The subject's refusal to comply with the Agent's command to surrender, his disabling attack upon one Agent, and his apparent intention to attack another, creates a reasonable belief that he poses an imminent threat of death or serious physical injury, justifying the use of deadly force to eliminate that threat. In the face of the imminent danger, Agents are not required to assume the risk of being incapacitated as a result of a physical confrontation with the subject, rendering the Agents incapable of protecting themselves and making their firearms accessible to the assailant.

SCENARIO #7: UNARMED, RESISTING

Agents attempt to execute an arrest warrant for an Unlawful Flight to Avoid Prosecution (UFAP)- Murder subject in the break room of the manufacturing plant where the subject works. They approach the subject and announce their identity and purpose. There is no reason to believe that he is presently armed with a deadly weapon. However, as soon as the Agents attempt to effect the arrest, the subject spits in the face of one of Agents, then grabs a nearby supporting column, wrapping it with his arms and legs. The Agents try to peel the man away from the column, but without success. The subject continues to spit and curse at the Agents. One Agent draws his handgun and informs the subject that if he doesn't let go of the column and surrender by the count of ten, he will be shot. The subject ignores the commands and continues cursing the Agents. At the count of ten the Agent fires.

DISCUSSION: The use of deadly force violates policy

It is not reasonable for the Agents to believe that the subject poses an imminent threat of death or serious physical injury to the Agents at present. Policy requires that they use non-deadly force to resolve this situation. This does not suggest that they should view the subject as harmless or as one who could not become a threat. As with any suspect or arrestee, Agents must be alert to the possibility that an imminent danger of death or serious physical injury may arise; but until such time as it does, deadly force is not an option.

SCENARIO #8: DANGEROUS, ESCAPING

FBI Agents are looking for a fugitive who jumped bail rather than face trial for distribution of cocaine. Two Agents go to the residence of the ex-wife of the fugitive, hoping to interview the woman about her former spouse's present address. As the Agents approach the house from the street, the fugitive emerges from the front door, sees the Agents and draws a handgun from the waistband of his pants. The Agents take cover behind the cars parked at the curb, draw their weapons and shout, "FBI! Put your hands up!" The fugitive opens fire, and begins to run across the front yard to get away. As the fugitive turns the corner of the house he trips over a bicycle and is seen to lose his gun. Regaining his feet, he runs along a driveway toward the back yard and begins to climb a chain link fence. One of the Agents yells for him to stop. When the fugitive ignores the command and continues to climb, the Agent fires a shot striking the fugitive.

DISCUSSION: The use of deadly force is permissible

It is reasonable for the Agents to believe that the subject of the force poses an imminent threat of death or serious physical injury. The subject's efforts to escape from the vicinity of a violent confrontation in which he inflicted or attempted infliction of death or serious physical injury supports a reasonable belief that he poses an imminent danger of death or serious physical injury to the Agents or others. Moreover, the subject has demonstrated his dangerousness by firing upon the Agents. Even though the fugitive was seen to have lost his gun, the Agents should consider the possibility that the suspect possesses another weapon. Agents are not required to pursue a demonstrably dangerous subject who has just attempted to kill them. The subject ignored commands to surrender. It is neither safe nor reasonable to require Agents to attempt to physically overpower a person who has demonstrated that he will use violence to avoid capture. To do so exposes the Agents' firearms to the subject and the Agents to unnecessary risk.

SCENARIO #9: ARMED, RESISTING

Agents have a warrant to arrest a man for a bank burglary that occurred several weeks previously. Unable to locate the subject at his apartment, they go to a nearby garage where he works as an auto mechanic. The Agents approach the subject, identify themselves, and tell him that he is under arrest. The subject glares at the Agents for a moment and then suddenly hurls a wrench at them which they manage to dodge. The subject then removes a small canister from a nearby bench and shouts, "If you guys don't get out of my way I'll mace you!" The Agents hold their positions about 30 feet from the subject, draw their handguns and order the subject to drop the canister. The subject does not comply with the command, but continues to point the canister in the Agents' direction as he moves toward them. When the subject is within about 20 feet of the Agents, they fire, striking the subject in the chest.

DISCUSSION: The use of deadly force is permissible

It is reasonable for the Agents to believe that the subject poses an imminent threat of death or serious physical injury to the Agents by his violent resistance to arrest with what appears to be a chemical agent. A non-compliant subject who has the capability of rendering Agents incapable of defending themselves also has the capacity to gain access to the Agents' weapons and to kill or seriously injure them. The Agents commanded the subject to drop the canister and surrender; he refused to do so, and increased the danger to the Agents by advancing toward them in a threatening manner. The Agents are not required to retreat from their duty or to permit the subject to get close enough to use what is believed to be an incapacitant against them.

SCENARIO #10: UNARMED, NON-DANGEROUS, ESCAPING

Agents possess a warrant to arrest a man for Interstate Transportation of Obscene Material. The Agents go to the subject's residence to execute the warrant. As they walk up the walkway to the front door, they hear the noise of a door slamming from the rear of the house, and they see a man matching the description of the subject running from the back of the house toward nearby woods. The Agents immediately give chase, but are unable to close the gap. Finally, one of the Agents shouts, "FBI! Stop or we'll shoot!" When the subject continues to flee, the Agent draws his handgun and fires a shot into the air. The subject continues to run, and just before he disappears into the woods, the Agent fires a second shot, striking the subject in the back.

**DISCUSSION: The use of deadly force violated policy
 The use of a warning shot violated policy**

It is not reasonable for the Agents to believe that the subject of the force poses an imminent threat of death or serious bodily injury. Deadly force is not permissible solely to prevent the escape of an individual. The subject in this scenario merely appears to be attempting to escape. Furthermore, the warning shot fired by one of the Agents violates the deadly force policy. If non-deadly force is not successful in effecting the subject's arrest, he will avoid arrest for the time being.

SCENARIO #11: DANGEROUS, ESCAPING

Agents attempt to execute arrest warrants on two subjects who have committed a series of bank and armored car robberies during which they killed or injured several people. The subjects immediately engage the Agents in a firefight during which two Agents are killed and five others are seriously injured. The two subjects, both of whom have also sustained gunshot wounds but are not incapacitated, attempt to escape in a nearby Bureau car. One of the Agents, himself seriously wounded, fires several shots into the passenger compartment of the vehicle, striking and killing the two subjects.

DISCUSSION: The use of deadly force is permissible

It is reasonable for the Agents to believe that the subjects of the force pose an imminent threat of death or serious physical injury. The subjects are fleeing the scene of a violent confrontation in which they have inflicted or attempted the infliction of death or serious physical injury. It is reasonable for the Agents to believe that as they attempt to escape the scene of that violent confrontation, they will continue to pose an imminent danger of death or serious physical injury to the Agents or others.

SCENARIO #12: ARMED, ESCAPING, RISKS TO OTHERS

Agents respond to an alarm indicating a bank robbery in progress. When they arrive on the scene, they observe a masked individual running from the bank with what appears to be a gun in his hand. The Agents identify themselves and order the subject to stop. In response, the subject fires two shots in the direction of the Agents. As the Agents dive for cover, the subject flees into a nearby crowded restaurant. An Agent pursues the subject, and from the entrance to the restaurant sees the subject making his way through the crowd toward the rear exit. The Agent fires at the subject.

DISCUSSION: The use of deadly force violates policy

It is reasonable to believe that the subject poses an imminent danger of death or serious physical injury. The subject is attempting to flee the scene of a violent confrontation where he just inflicted or attempted the infliction of death or serious physical injury. However, the firing of the weapon by the Agent into a crowded restaurant creates an unreasonable danger to the public that is not outweighed by the likely benefits. The Agents presented with that unreasonable risk to the public must permit the subject to escape. In considering the availability of other options, Agents are reminded that pursuing an armed and dangerous subject under the circumstances presented poses an unreasonable risk to the Agents and, under the policy, Agents are not required to assume unreasonable risks.

SCENARIO #13: ARMED, DANGEROUS, ESCAPING

Agents are involved in executing an arrest warrant on a man who has committed a series of bombings over a period of years resulting in several deaths and serious injuries. There is no information to suggest that the subject carries firearms or other weapons. When the Agents approach the subject, he sees them from a distance of about 25 yards and quickly turns and runs in the opposite direction. The Agents shout, "FBI! Stop!" Ignoring the commands, the subject continues to run. When it becomes apparent that the Agents cannot overtake the subject, one Agent again shouts, "FBI! Stop or I'll shoot!" When the subject continues his flight, the Agent fires two rounds, striking him in the back.

DISCUSSION: The use of deadly force violates policy

Although the subject's prior crimes justify the belief that he is dangerous, it is not reasonable to believe that he poses an imminent danger to the Agents or to others as defined under the deadly force policy. Neither the egregious nature of his crimes nor the probability that he will continue his dangerous acts unless captured satisfies the imminent danger requirement of the policy. In the absence of an imminent danger, deadly force is not justified.

SCENARIO #14: ARMED, DANGEROUS

Agents possess a warrant to arrest a subject for armed robbery of a bank the day before. During the robbery, the subject shot and wounded a bank guard. As the Agents drive into the neighborhood where they believe the subject previously resided, they observe a man matching the subject's description walking down the sidewalk. From a distance of about 25 yards the Agents see what appears to be a handgun tucked into the waistband of the subject's pants. Getting out of their cars, the Agents walk toward the subject. When they are about 10 yards from the subject, one of the Agents shouts, "FBI! Put up your hands! We have an arrest warrant!" Following a quick glance in the direction of the Agents, the subject turns and runs away from the Agents and toward a nearby house. The Agent shouts, "FBI! Stop or I'll shoot!" When the subject continues to run, the Agent fires at the subject.

DISCUSSION: The use of deadly force is permissible

It is reasonable to believe that the subject of the force poses an imminent threat of death or serious physical injury to the Agents or others he may encounter. The Agents have a reasonable belief that the subject that they are attempting to arrest is presently armed with a firearm. If the subject reaches the house under that circumstance, he will have the tactical advantage of cover, whereas the Agents are in an exposed position. In addition, the subject poses a danger to other persons in the house whom he may take as hostages or otherwise injure. The nature and imminence of the danger permits the use of deadly force under those circumstances. Since permitting the subject to enter the house would place the Agents and others in imminent danger, deadly force is permissible.

APPENDIX G: (U) CLASSIFIED PROVISIONS

(U) See the separate classified DIOG Appendix G.

APPENDIX H: (U) PRE-TITLE III ELECTRONIC SURVEILLANCE (ELSUR) SEARCH POLICY

H.1 (U) SCOPE

(U) 18 U.S.C. § 2518(1)(e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. The below policy is designed to conform with this statutory requirement, clarify any past confusion, and address the effects on the previous search policy resulting from the recent elimination of the requirement for an agency Action Memorandum by the Office of Enforcement Operations (OEO). This policy supersedes the March 5, 2003 Director’s Memorandum to All Special Agents in Charge Re: Pre-Title III Electronic Surveillance (ELSUR) Search Policy, and the April 14, 2008, All Field Offices EC from RMD, Case ID# 321B-HQ-C1186218.

H.2 (U) REVISED POLICY

H.2.1 (U) COMPLIANCE WITH THE PREVIOUS APPLICATION PROVISION

(U) 18 U.S.C. § 2518(1)(e) requires that each application for an order to intercept wire, oral, or electronic communications (hereinafter “Title III”) contain a statement describing all previous applications for Title III surveillance of the same persons, facilities, or places named in the current application. Although a failure to comply with § 2518(1)(e) will not always result in suppression of evidence, deliberate noncompliance likely will.

(U) To comply with this requirement, FBI search policy requires that a “search,” i.e., an automated indices search, of the FBI’s ELSUR Records System (ERS) be conducted prior to filing a Title III affidavit and application with the court. To assist field offices in conducting appropriate searches, the following guidelines are provided.

H.2.1.1 (U) WHEN TO SEARCH

- A) (U) ELSUR SEARCHES: ELSUR searches for both sensitive and nonsensitive Title IIIs, including applications not requiring the approval of the Department of Justice (DOJ), Office of Enforcement Operations (OEO), such as for a digital display pager, must be conducted not more than 45 calendar days prior to the date the application and affidavit are filed with the court.
- B) (U) SPIN-OFFS: A “Spin-off” is a new application to begin surveillance at additional facilities arising from an existing investigation in which one or more Title IIIs have already been authorized. A spin off is considered to be an “original” request, even though some or all of the named persons are also named in the prior Title IIIs. As with any new Title III, a search of the persons, facilities, and/or places specified in the “spin-off” application must be conducted not more than 45 calendar days prior to the date the application and affidavit are filed with the court.
 - 1) (U) Any of the persons, facilities, and/or places named in the “spin-off” application and affidavit which have been the subject of a previous search conducted not more than 45

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

calendar days prior to the date the application and affidavit are filed with the court need not be searched again. However, a copy of the EC documenting the results of the previous search must be serialized in the investigative file to which the “spin-off” relates and in the corresponding ELSUR Administrative Subfile.

- C) (U) EXTENSIONS: When an extension is sought, newly identified persons, facilities, and/or places must be searched not more than 45 calendar days prior to the date the application and affidavit are filed with the court.
- 1) (U) If an individual named by a partial name, nickname, street name, and/or code name is subsequently identified by at least a first initial and a last name, a search must be conducted for the now-identified individual prior to seeking an extension naming that person.
 - 2) (U) The same persons, facilities, and/or places previously searched that are named in an extension application and affidavit need not be searched again unless the original intercept has continued beyond 120 calendar days. When a Title III intercept extends beyond 120 calendar days from the date of the original order, an additional search of the persons, facilities, and/or places named in the request for extension must be conducted.

H.2.1.2 (U) HOW TO SEARCH

(U) The ERS must be searched for previously submitted Title III applications to intercept communications involving any of the persons, facilities, and/or places specified in the current Title III application.

- A) (U) PRIOR APPLICATIONS: Searches are required only for previously submitted applications. There is no obligation to search for prior interceptions. The ELSUR search will provide records of the persons, facilities, and/or places named in prior applications filed by the FBI and other federal law enforcement agencies named in the request. Any prior applications identified must be set forth in the affidavit in support of the new application.
- B) (U) PRIOR INTERCEPTIONS: If information regarding earlier interceptions is desired, an Agent may request a search of “all records” for any or all of the persons, facilities, and/or places named in the search request. A search for “all records” will include prior FBI intercepts occurring over Title III and consensual monitoring in criminal matters. This information may be relevant to the “necessity” portion of the affidavit, if an agent has reason to believe there were numerous previous interceptions.

H.2.1.2.1 (U) PERSONS

(U) List the true names or best known names of individuals for whom there is probable cause to believe that: (1) they are involved in the specified criminal activity, or (2) their criminal communications are expected to be intercepted over the target facility or within the target premises.¹ When the involvement of a particular individual in the offense is not clear, Agents should err on the side of caution and name that individual in the affidavit.

¹ (U) All individuals listed in the application and affidavit as being involved in the specified criminal activity should be searched in ERS, not just those individuals who are expected to be intercepted. Further, the ELSUR Operations Technician is required to index into ERS all names listed in the application, which would include individuals who are involved in the specified criminal activity, regardless of whether they are expected to be

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

- A) (U) A minimum of a first initial and last name is required for an ERS search. Biographical data such as date of birth, FBI Number, and/or Social Security Account Number, if known, must be included. Do not include partial names, nicknames, street names, and/or code names. Include aliases only if the true name is unknown or if the alias meets ELSUR search requirements. For example, if the alias is a full name alias, it should be included (i.e., John Smith a/k/a "William Johnson" or William Smith a/k/a "Liam Smith").
- B) (U) Persons not fully identified by a first initial and a last name who are specific targets of the interception should be named "John Doe," "Jane Doe," or "FNU LNU" and so listed as a "Person" whose communications are expected to be intercepted over the target facility. Such names (John Doe, Jane Doe, FNU LNU) need not be the subject of an ELSUR search. If such an individual is later identified, the Agent must so advise the ELSUR Operations Technician (EOT) to allow the "John Doe," "Jane Doe," or "FNU LNU" ELSUR record to be appropriately modified for retrieval in subsequent ELSUR searches.
- C) (U) A search of the ERS must be conducted for the subscriber or service provider of the target facility only if the subscriber or service provider is believed to be involved in the specified criminal offense(s).
- D) (U) Any additional persons, facilities, and/or persons mentioned in the affidavit, but not also specified in the application as a person, facility, and/or place for which authorization to intercept is being sought, need not be searched or listed in the FD-940 (Pre-Title III ELSUR Search Request).

H.2.1.2.2 (U) FACILITY

(U) List available numeric and/or alphanumeric values directly associated with the device, equipment, or instrument over or from which the subjects are communicating (e.g., a telephone, pager, computer, etc.). Such values may include, but are not limited to, the telephone number of a land line phone, cell phone, or pager, Personal Identification Number, Cap Code, Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI) Number, International Mobile Equipment Identifier (IMEI) Number, and/or Internet account information (including but not limited to screen name, online identity, ICQ number, and/or IP address).

- A) (U) Names of businesses, organizations, or agencies must be searched only if there is probable cause to believe the business, organization, or agency is culpable in the specified criminal offense(s).
- B) (U) Searches need not be conducted for telephone numbers or other facilities subscribed to, leased, or owned by the FBI for use in the investigation for which the ELSUR is being sought.

H.2.1.2.3 (U) PLACES

(U) List: (1) each address of a targeted landline phone or computer terminal which will be subject to the Title III order, and/or (2) sufficient information to describe or identify each physical location where a microphone surveillance (MISUR) installation will be located (e.g., vehicle identification number, license number, serial number of a boat or plane, and/or the

intercepted over the target facility or within the target premises. These names are to be indexed as Principal records.

address of a residence or a business for a fixed ELSUR installation). Do not include addresses of subscribers or proprietors of mobile installations such as cell phones, pagers, vehicles, boats or planes, etc.

(U) Persons, facilities, and/or places added to the affidavit subsequent to the Chief Division Counsel's (CDC) review, or the review of any other reviewing or approving official, must be searched prior to submitting the affidavit to the court. The responsible AUSA should be asked whether additions have been made to the affidavit without the FBI's knowledge.

H.2.1.3 (U) WHERE TO SEARCH

(U) A search of the FBI's ERS must be conducted for each item named in the search request. A search of the Drug Enforcement Administration (DEA) and Immigration and Customs Enforcement (ICE) ERS is required for all Title 21 predicate offenses. As a matter of policy, a DEA and ICE ELSUR search is automatically conducted by FBIHQ for all 245 and 281 investigative classifications, and any other application involving a Title 21 offense.

- A) (U) The ERS of any other federal, state, or local law enforcement agency that is actively participating in a joint investigation (as opposed to mere task force participation) or as to which there is reason to believe may have previously sought to intercept wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified in the instant application, should be searched. Where a search of state and/or local law enforcement ELSUR records is requested, the request should include a point of contact from the outside agency, if known.
- B) (U) If there is reason to believe that any of the persons, facilities, and/or places specified in the current application have been the target of Title III electronic surveillance by another federal agency, that agency must be requested to conduct an ELSUR search of its records.

H.2.1.4 (U) HOW TO INITIATE A SEARCH REQUEST

(U) Form FD-940 (Pre-Title III ELSUR Search Request) is used for requesting pre-Title III ELSUR searches of the ERS of the FBI and any other federal, state, or local law enforcement agency. Each search request should state whether it is for:

- A) (U) An initial search, first filing;
- B) (U) An initial search of newly named persons, facilities, and/or places for an extension;
- C) (U) An initial search of newly named persons, facilities, and/or places for a "spin-off" wiretap;
or
- D) (U) A 120-calendar day search (recheck) for a continuing wiretap.

(U) The form is designed to assist personnel requesting a search by guiding them through the process. Use of the form will ensure search requirements are met.

(U) If an emergency situation exists, as defined by 18 U.S.C. § 2518(7), an ELSUR search may be requested telephonically to the field office EOT.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

H.2.1.4.1 (U) SEARCH PROCEDURE

(U) The EOT will conduct a search of the ERS for records of “previous applications only” or “all records” as specified in the FD-940. Records retrieved as a result of the search will be furnished to the requesting Agent. If intercept records are requested for any or all of the persons, facilities, and/or places named in the FD-940, intercept records which relate to unclassified criminal matters will be printed in their entirety and furnished to the requesting Agent as an enclosure to an EC documenting the search.

(U) It is the responsibility of the requesting Agent to use reasonable efforts to determine whether the persons, facilities, and/or places identified in the search are the same persons, facilities, and/or places specified in the current application. If there is reason to believe they are, offices identified as having filed previous applications must be contacted and the EOT in that office must be asked to review the pertinent ELSUR file to determine whether the persons, facilities, and/or places identified in the search are, in fact, the same as those specified in the current application.

(U) It is not necessary to contact other offices regarding common names for which no special identifying data is available unless there is reason to believe there is a nexus between the current investigation and the investigation conducted by the other field offices.

(U) Documentation confirming the conduct of all pre-Title III ELSUR searches must be uploaded and filed in the investigative file or the corresponding ELSUR Administrative (ELA) Subfile.

H.2.1.5 (U) WHAT TO SAY

A) (U) NO PREVIOUS APPLICATIONS: Sample proposed affidavit language when no previous applications have been filed:

- 1) (U) “Based upon a search of the records of the Federal Bureau of Investigation (and any other agency requested), no previous applications have been filed for an order authorizing the interception of wire, oral, or electronic communications involving any of the persons, facilities, and/or places specified herein for which authorization to intercept is being sought.”

B) (U) PREVIOUS APPLICATIONS:

- 1) (U) If there was a previous application, include all relevant information concerning such application in the affidavit in support of the current application. Identify the persons, facilities, and/or places named, the method(s) of interception sought, the date the order was granted or denied, the court that issued or denied the order, the name of the authorizing or denying judge, the judicial district in which the application was filed, and the relevance, if any, of the previous application to the current investigation.
- 2) (U) Sample proposed affidavit language when previous applications have been filed: “John Doe was named in a previous application for an order authorizing the interception of wire and electronic communications. The order was signed on (date), by U.S. District Judge (name), of the District of (State), authorizing the interceptions for a period of thirty (30) days. An extension of the order was signed by Judge (name) on (date), authorizing the continued interception for an additional 30-day period.” (Include relevance, if any, of the previous applications to the current investigation).

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

H.2.1.6 (U) DOCUMENTATION

- A) (U) Agents must provide a copy of the following to the field offices's ELSUR Operations Technician (EOT):
- 1) (U) signed application, order and supporting affidavit;
 - 2) (U) completed CDC Checklist (FD-926);
 - 3) (U) EC signed by the appropriate approving official (SAC or designee or appropriate HQ official) documenting approval to seek court authorization for the Title III application; and
 - 4) (U) DOJ Memorandum directed to the AUSA entitled "Authorization for Interception Order Application."
- B) (U) The EOT and the ELSUR supervisor are responsible for confirming that ELSUR searches were properly conducted as set forth in the final applications submitted to the court. Because this review is not conducted until after the application and order have been submitted to the court, the SA and SSA are responsible for verifying that all required ELSUR searches have been conducted prior to submission of the application and affidavit to the court. The EOT is responsible for forwarding a copy of each final application, the SAC or HQ approving EC, and the DOJ Memorandum via Title III Cover Sheet to the Policy and Compliance Unit (PACU) of the Records Management Division (RMD) immediately upon the entry of Principal and Proprietary Interest Records into the ERS.
- C) (U) Macro EC Form FD-940 (Pre Title III ELSUR Search Request) must be used when requesting a search of any federal, state, or local law enforcement agency's ELSUR Records System (ERS), including the FBI's. When an Agent requests a search of a state or local law enforcement agency's records, the macro will produce an "auxiliary" letter simultaneously. The auxiliary letter will include only that information necessary to conduct the local search and should be disseminated by the field office to the respective state or local agency.
- D) (U) All requests for ELSUR searches must be uploaded and filed in the corresponding ELSUR Administrative (ELA) Subfile and submitted with adequate time for the EOT to conduct the search and document the results. It is the responsibility of the affiant and the affiant's supervisor to ensure that all ELSUR checks have been properly completed prior to submission of the application and affidavit to the court.

APPENDIX I: (U) ACCESSING STUDENT RECORDS MAINTAINED BY AN EDUCATIONAL INSTITUTION (“BUCKLEY AMENDMENT”)

I.1 (U) SUMMARY

(U) The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. § 1232g, as amended by Public Law 107-56 (USA Patriot Act)), commonly referred to as the “Buckley Amendment,” restricts the ability of educational agencies or institutions (collectively “schools”) to release educational records or personally identifiable information contained in such records without the consent of the student or the student’s parent.

(U) FERPA defines “education records” as those records, files, documents and other materials which:

- A) (U) contain information directly related to a student; and
- B) (U) are maintained by an educational agency or institution or by a person acting for such agency or institution. (20 U.S.C. § 1232g(a)(4)(A)(i)).

(U//FOUO) If operationally feasible, FBI employees should request the consent of the student or parent, as appropriate, in order to obtain covered records. During an Assessment, the FBI may ask school officials to provide certain information without the consent of the student or parent (see Section 18.5.6); during a Predicated Investigation, the FBI may compel production of education records, as set forth below.

I.2 (U//FOUO) ACCESSING STUDENT INFORMATION OR RECORDS DURING AN ASSESSMENT

(U//FOUO) During an Assessment, FBI employees may seek **voluntary disclosure** of certain student records and information about students from schools without the consent of the student or parent.

I.2.1 (U) DIRECTORY INFORMATION

(U//FOUO) “Directory information” is information contained in an education record of a student “that would not generally be considered harmful or an invasion of privacy.” (34 C.F.R. § 99.3) Specifically, “directory information” includes, but is not limited to: the student’s name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status (e.g., undergraduate or graduate, full-time or part-time), participation in officially recognized activities or sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended. A school may disclose “directory information” from its records without prior consent if: (1) it has a directory information policy to disclose such information and (2) it has provided its students notice of the policy and the opportunity to opt out of having “directory information” disclosed. (See 34 C.F.R. § 99.37)

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) The scope of information that can be released as directory information may be narrowed by the school. For instance, if a college chooses not to categorize students' names and addresses as directory information, it must not voluntarily disclose such information to the FBI (*Krauss v. Nassau Community College*, 469 N.Y.S. 2d 553 (N.Y. Sup. 1983)). Schools are also required to afford students (or parents, if the student is under 18) the opportunity to prohibit the release of directory information without their prior consent (or a court order). *Note*: the Buckley Amendment *permits* schools to release directory information (absent an objection from the student); it does *not require* them to do so. Directory information may be sought orally or in writing.

1.2.2 (U) OBSERVATIONS

(U//FOUO) FERPA governs the release of educational records. It does not govern the release of information gathered by a school official, based on his or her own observations. Accordingly, notwithstanding Buckley, a school official may disclose activity or behavior observed by the official.

1.2.3 (U) LAW ENFORCEMENT UNIT RECORDS

(U//FOUO) Under FERPA, schools may disclose information from "law enforcement unit records" without the consent of the parent or student. This exemption is limited to records that a law enforcement unit of a school creates and maintains for a law enforcement purpose. "Law enforcement record" is narrowly defined as a record that is: (i) created by the law enforcement unit; (ii) created for a law enforcement purpose; and (iii) maintained by the law enforcement unit. (34 C.F.R. § 99.8(b)) If another component of the school discloses a student education record to the school's law enforcement unit, that record is not a "law enforcement unit record" because it was not *created* by the law enforcement unit. Thus, a law enforcement unit cannot disclose, without student consent, information obtained from education records created by other component of the school, even if the record has been shared with the law enforcement unit.

1.2.4 (U) HEALTH OR SAFETY EMERGENCY

(U//FOUO) FERPA does not restrict the disclosure of educational records in connection with a health or safety emergency. The regulations provide that schools may disclose information from an education record "to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals" and that the exception is to be "strictly construed." As is the case with other emergency disclosure provisions (see 18 U.S.C. § 2702), it is up to the school to determine in the first instance whether disclosure is necessary to protect the health or safety of the student or another individual. If it makes that determination, it is permitted to disclose educational records voluntarily and without the consent of the student or parent.

1.2.5 (U) NON-STUDENTS

(U//FOUO) FERPA governs records of "students." A "student" is defined as a person on whom a school maintains educational records or personally identifiable information but does not include someone who has not attended that school. Files retained on rejected applicants may be provided without prior permission or notification. (*Tarka v. Franklin*, 891 F.2d 102 (5th Cir. 1989))

I.3 (U//FOUO) ACCESSING STUDENT INFORMATION OR RECORDS IN PREDICATED INVESTIGATIONS

(U//FOUO) In addition to seeking voluntary production of records that can be voluntarily produced (see I.2 above), in a Predicated Investigation, FBI employees may **compel production** of education records without notice to the student or the student's parents as follows:

I.3.1 (U) FEDERAL GRAND JURY SUBPOENA

(U//FOUO) Schools shall disclose education records in response to a federal grand jury subpoena. In addition, the court may order the institution not to disclose to anyone the existence or contents of the subpoena or the institution's response. If the court so orders, then neither the prior notification requirements of 34 C.F.R. § 99.31(a)(9) nor the recordation requirements at 34 C.F.R. § 99.32 would apply (see DIOG Section 18.6.5).

I.3.2 (U) ADMINISTRATIVE SUBPOENAS

(U//FOUO) Schools may disclose education records in response to an administrative subpoena. Administrative subpoenas may be issued in narcotics investigations (see DIOG Section 18.6.4.3.2.1), sexual exploitation or abuse of children investigations (see DIOG Section 18.6.4.3.2.2), and health care fraud investigations (see DIOG Section 18.6.4.3.2.3). As with federal grand jury subpoenas, the issuing agency may, for good cause shown, direct the school not to disclose the existence or contents of the subpoena or the institution's response. If the subpoena includes a nondisclosure directive, the school is permitted to request a copy of the good cause determination.

I.3.3 (U) FISA ORDER FOR BUSINESS RECORDS

(U//FOUO) See DIOG Section 18.6.7.

I.3.4 (U) EX PARTE ORDERS

(U//FOUO) The USA Patriot Act amended FERPA to permit schools to disclose personally identifiable information from the student's education records to the Attorney General or his designee without the consent or knowledge of the student or parent in response to an *ex parte* order issued in connection with a terrorism investigation. Such disclosures are also exempt from the Buckley Act requirements that disclosure of information from a student's records be documented in the student's file.

APPENDIX J: (U) INVESTIGATIVE FILE MANAGEMENT AND INDEXING

J.1 (U) INVESTIGATIVE FILE MANAGEMENT

J.1.1 (U) OFFICE OF ORIGIN (OO)

(U//FOUO) Generally, the Office of Origin (OO) is determined by:

- A) (U//FOUO) The residence, location or destination of the subject of the investigation;
- B) (U//FOUO) The office in which a complaint is first received;
- C) (U//FOUO) The office designated by FBIHQ as OO in any investigation;
- D) (U//FOUO) The office in which the Foreign Police Cooperation investigation is opened (163 classification);
- E) (U//FOUO) The office in which the Domestic Police Cooperation investigation is opened (343 classification);
- F) (U//FOUO) The office in which the recovery of the vehicle occurred in an Interstate Transportation of Stolen Motor Vehicles (ITSMV) investigations;
- G) (U//FOUO) The office in which the contempt of court occurred;
- H) (U//FOUO) The office in which there is a violation of an order, judgment, or decree issued from any judicial district in an FBI civil Racketeer Influenced and Corrupt Organizations (RICO) investigation;
- I) (U//FOUO) The office in which the subject was convicted in investigations involving parole, probation, and mandatory release violators;
- J) (U//FOUO) The office in which the escape occurred, in Escaped Federal Prisoner and escaped deserter investigations;
- K) (U//FOUO) The New York Field Office in courier investigations;
- L) (U//FOUO) FBIHQ in all applicant, Background Investigation - Pardon Attorney's Office (73 classification) investigations;
- M) (U//FOUO) FBIHQ in OPM security referral (140A and 140C classification) investigations;
- N) (U//FOUO) FBIHQ, Counterterrorism Division (CTD), Counterterrorism Watch Unit in all Counterterrorism Major Cases (900 classification);
- O) (U//FOUO) FBIHQ, Critical Incident Response Group (CIRG) in all National Center for the Analysis of Violent Crime (NCAVC) cases (252A through 252E classifications); and
- P) (U//FOUO) FBIHQ, Office of Professional Responsibility (OPR) in OPR investigations (263 classification).

(U//FOUO) When special circumstances exist, however, the origin may be assumed by the field office which has the most compelling interest. Uncertainties and disagreements must be resolved by the appropriate FBIHQ operational division.

J.1.2 (U) INVESTIGATIVE LEADS AND LEAD OFFICE (LO)

(U//FOUO) Leads are sent by EC, or successor document (hereafter referred to as EC), to offices and assigned to individuals/organizations in order to aid investigations. When the OO sets a lead to another office, that office is considered a Lead Office (LO).

(U//FOUO) There are only two types of investigative leads: “Action Required” and “Information Only.”

J.1.2.1 (U) ACTION REQUIRED LEAD

(U//FOUO) An action required lead must be used if the sending office requires the receiving LO to take some type of investigative action.

(U//FOUO) An action required lead may only be set by EC out of an open investigative file, including an:

- A) (U) Assessment file, including a zero sub-assessment file;
- B) (U) Predicated Investigation file;
- C) (U) pending inactive investigation file; or
- D) (U) unaddressed work file.

(U//FOUO) An action required lead cannot be set out of a closed investigative file, a zero (0) or double zero (00) file.

(U//FOUO) An action required lead must be assigned, and it must be covered before the underlying investigation has been completed/closed.

J.1.2.2 (U) INFORMATION ONLY LEAD

(U//FOUO) An information only lead must be used when no specific action is required or necessary from the receiving LO.

(U//FOUO) An information only lead may be set by EC out of an opened or closed investigative file, including a:

- A) (U) zero (0) file;
- B) (U) double zero (00) file;
- C) (U) Assessment file, including a zero sub-assessment file;
- D) (U) Predicated Investigation file;
- E) (U) pending inactive investigation file; or
- F) (U) unaddressed work file.

(U//FOUO) An information only lead does not have to be assigned in order to be covered, and they can be covered while they are in the “Set” status.

J.1.3 (U) OFFICE OF ORIGIN'S SUPERVISION OF CASES

(U//FOUO) The OO is responsible for proper supervision of Assessments and investigations in its own territory and being conducted in a LO. The FBI employee, usually an FBI Special Agent, to whom an investigation is assigned, is often referred to as the "Case Agent." An FBI employee is personally responsible for ensuring all logical investigation is initiated without undue delay, whether the employee is assigned in the OO or in an LO; this includes setting forth Action Required or Information Only leads as appropriate for other offices or other FBI employees in his/her own office. The OO Case Agent has overall responsibility for supervision of the investigation. When an LO has a delayed or delinquent investigation, it is the responsibility of the OO Case Agent to notify the LO (orally or in writing by email or EC, depending on the urgency of the situation) of its delinquency.

J.1.4 (U) INVESTIGATION AND OTHER FILES

(U//FOUO) There are several types of non-investigative files used in the FBI, including zero files, double zero files, administrative files, and control files. Additionally, there are several types of investigative files used in the FBI, including zero sub-assessment files, Preliminary Investigation files, Full Investigation files, Full Enterprise Investigation files, positive foreign intelligence Full Investigation files, and unaddressed work files. FBI files may be opened, closed, or placed in pending inactive status as specified below. Note that in each of these files, all communications related to previous communication must note the existing communication's ACS, or successor case management system, and Universal Index serial numbers in the reference fields.

(U//FOUO) Certain records may be restricted based on the classification of the records, e.g., on the sensitivity of the investigation. See the Corporate Policy Directive 243D, dated October 13, 2009.

(U//FOUO) The types of files are:

J.1.4.1 (U) ZERO "O" FILES

(U//FOUO) Zero files may be opened in all file classifications. Zero files may contain leads, complaints not initiated as Assessments or Predicated Investigation, or other documents that do not require investigation. The documents contained within a zero file must be serialized. When additional communications referring to the same subject are received, they must be linked to the prior communication by placing the serial number of the prior communication in the reference field when the communication is uploaded and serialized in the Electronic Case File (ECF) of ACS, or successor case management system. Because a zero file contains material which does not require investigation, Action Required leads cannot be set out of zero files. Only Information Only leads can be set out of zero files.

J.1.4.2 (U) DOUBLE ZERO "OO" FILES

(U//FOUO) Double Zero files may be opened in all file classifications. Double Zero files may contain documentation, such as instructions, policy, statutes, and decisions applicable to the classification, that do not require investigation. The documents contained within a double zero file must be serialized. When additional communications referring to the same subject are

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Domestic Investigations and Operations Guide

received, they must be linked to the prior communication by the reference field in the Electronic Case File, ACS, or successor case management system. Because a Double Zero file contains material which does not require investigation, Action Required leads cannot be set out of double zero files. Only Information Only leads can be set out of double zero files.

J.1.4.3 (U) ADMINISTRATIVE "A" FILES

(U//FOUO) Administrative files may be used only for administrative purposes; they may not be used for investigative purposes. Administrative files may be used for documenting non-investigative matters, such as training matters (1 classification), administrative matters (319 classification), personnel files (67 classification), etc. **Note: Investigative activity may not be documented in an administrative file.** Administrative files are designated with the letter "A" before the case number, e.g., 319X-HQ-A12345.

(U//FOUO) Administrative (non-investigative) Leads may be assigned out of administrative files. When referring to the file number of an administrative file in communications, the file number must include the letter "A" as part of the case number to indicate the file is an administrative file.

J.1.4.4 (U) CONTROL "C" FILES

(U//FOUO) Control files are separate files established for the purpose of administering investigative programs. Control files are opened at the discretion of the individual responsible the investigative program. Control files may be opened in all classifications.

(U//FOUO) Like administrative files, control files may be used only for administrative purposes. Control files may be used for documenting program management communications, policy pronouncements, technical or expert assistance to another law enforcement or intelligence agency, or other administrative/managerial functions. Administrative/managerial functions could include liaison contacts, training exercises, training received/provided, etc. **Note: Investigative activity may not be documented in a control file.** Administrative (non-investigative) leads can be assigned out of control files.

(U//FOUO) Control files are designated with the letter "C" before the case number, e.g., 29B-NF-C4456. When referring to the file number of a control file in communications, the file number must include the letter "C" as part of the case number to indicate the file is a control file.

J.1.4.5 (U) INVESTIGATIVE FILES

J.1.4.5.1 (U) ASSESSMENT FILES

J.1.4.5.1.1 (U) ZERO SUB-ASSESSMENT FILES (FOR TYPE 1 & 2 ASSESSMENTS)

(U//FOUO) Zero sub-assessment files exist for all investigative classifications and are used to store all information acquired during these Assessments. Type 1 & 2 Assessments must be filed in an applicable zero sub-assessment file (e.g., 91-0-ASSESS-D, 15-0-ASSESS) when completed. When completing the FD-71 or Guardian lead for an

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Assessment involving a sensitive investigative matter, the FBI employee must select the option “Sensitive Investigative Matter.”

(U//FOUO) Action leads can be set when using a zero sub-assessment file.

(U//FOUO) Guardian may be used only for documenting those Assessments described in DIOG Section 5.6.3.1 regarding international terrorism, domestic terrorism, weapons of mass destruction terrorism, and cyber terrorism. The FD-71 or EC must be used to document all other Assessments, including criminal, counterintelligence, and non-terrorism WMD and Cyber. Both Guardian and the FD-71 provide the ability to set action leads.

J.1.4.5.1.2 (U) INVESTIGATIVE CLASSIFICATION ASSESSMENT FILES (FOR TYPE 3, 4 AND 6 ASSESSMENTS) AND POTENTIAL CHS FILES (FOR TYPE 5 ASSESSMENTS)

(U//FOUO) See DIOG Section 5 for the appropriate investigative file classification to be used when opening a Type 3, 4, 5, or 6 Assessment file.

(U//FOUO) Because these Assessments require prior supervisory approval, the file must begin with an opening EC (DIOG Section 5.6.3.2 through 5.6.3.5 type Assessments as discussed above). The title/caption of the opening EC must contain the word “Assessment,” and the synopsis must identify the purpose and the objective of the Assessment. If at the time of the opening, or at anytime thereafter, the Assessment involves a sensitive investigative matter, the title/caption must contain the words “Assessment” and “Sensitive Investigative Matter.” When the objective has been met, a closing EC must be approved by the SSA or SIA and uploaded to the file. If additional objectives arise during the Assessment, they must be documented in an EC, approved by the SSA or SIA, and uploaded to the file.

J.1.4.5.2 (U) PRELIMINARY AND FULL INVESTIGATION (PREDICATED) FILES

(U//FOUO) A Preliminary Investigation, Full Investigation, Full Enterprise Investigation, and Full Positive Foreign Intelligence Investigation must be initiated as discussed in DIOG Sections 6, 7, 8, and 9, respectively. Investigative information related to these investigations must be placed in the investigative file, spun-off, or referred to another agency as authorized.

J.1.4.5.3 (U) PENDING/INACTIVE FULL INVESTIGATION FILES

(U//FOUO) A Full Investigation may be placed in a pending-inactive status when all investigation has been completed and only prosecutive action or other disposition remains to be determined and reported, e.g., locating a fugitive outside the United States. The DIOG does not authorize placing a Preliminary Investigation in pending inactive status. A pending-inactive Full Investigation may be assigned to investigative personnel or a squad/unit.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

J.1.4.5.4 (U) UNADDRESSED WORK FILES

(U//FOUO) An Assessment or Full Investigation that cannot be adequately addressed by available human resources due to its relative lower priority can be placed in “Unaddressed Work” status, which is an “opened” file. The SSA must ensure that all reasonable investigative resources are being utilized on other investigative matters prior to designating an Assessment or Full Investigation as Unaddressed Work. Prior to placing a matter into Unaddressed Work status, personnel should review the appropriate FBIHQ division’s PG to ensure program procedures do not prohibit utilizing Unaddressed Work for a particular investigative classification. SSA/SIA review of Assessments or Full Investigations that are in Unaddressed Work status must adhere to DIOG Section 3.4.4 above, to determine whether the matter should remain in an Unaddressed Work status, or be closed, and whether there is any concurrent investigative jurisdiction. If concurrent jurisdiction exists, the matter must be referred in writing to the appropriate law enforcement agency within 180 days of making the determination that concurrent jurisdiction exists, unless such a referral would: (i) jeopardize an ongoing investigation; (ii) endanger the safety of an individual; (iii) identify a confidential human source (CHS); (iv) interfere with a CHS’s cooperation; or (v) reveal legally privileged information. If a referral is not made, the SSA must document the reason by EC in the appropriate file with a copy furnished to the appropriate operational unit.

(U//FOUO) Information or allegations regarding criminal activity which, if proven, would fall below the established prosecution guidelines of the relevant United States Attorney’s office and, as a result, are subject to blanket declinations should not be placed in Unaddressed Work status. These matters must either be opened in their respective substantive classification and then closed using “status” (C5) - USA Declination pursuant to a blanket declination letter or placed in the appropriate zero file. These matters may not be placed into an administrative “A” file or control “C” file.

(U//FOUO) Unaddressed Work “Control” files are not permitted. New Unaddressed Work must be opened and assigned a Universal Case File Number (UCFN). Unaddressed Work investigations must be opened with a investigation type of “U” (for unaddressed), assigned to the appropriate squad, and assigned a UCFN.

(U//FOUO) The FD-71 provides a mechanism to assign an Assessment to an Unaddressed Work file. In the FD-71, the Supervisor must select a reason for assigning the matter to the Unaddressed Work file and choose the appropriate classification. Upon uploading the FD-71, a new Unaddressed Work file will be opened. Guardian (FD-71a) does not have an “Unaddressed Work” option because Guardian leads cannot be placed in an Unaddressed Work status.

J.1.4.5.5 (U) SPIN OFF INVESTIGATION FILES

(U//FOUO) A spin-off investigation originates from an existing investigation. The spin-off investigation must have all the elements required to establish it as a separate investigation within the appropriate investigative classification.

J.2 (U) INDEXING - THE ROLE OF INDEXING IN THE MANAGEMENT OF FBI INFORMATION

(U//FOUO) The text of FBI-generated documents must be uploaded into the Electronic Case File (ECF) component of the ACS system to be searchable, retrievable, and sharable through automated means. A full text search of the ACS system's ECF identifies only information that is available electronically and does not search for information that may be contained in the FBI's paper records. Because some records are not uploaded into ACS, all records must also be indexed. Even if a document is uploaded into ACS it must be indexed. While the full text of uploaded documents can be electronically searched, many records checks are performed using the Universal Index (UNI), a sub-component of ACS, rather than a text search of ECF.

(U//FOUO) The purpose of indexing is to record individual's names; non-individual's names, such as corporations; and property which are relevant to FBI investigations so that this information can be retrieved, if necessary. The most common use of UNI is to respond to executive branch agencies' request name searches as part of their investigations to determine suitability for employment, trustworthiness for access to classified information and eligibility for certain government benefits. If employees do not properly index names and places that arise in FBI investigations, the FBI could provide erroneous information to other federal agencies. Further advice about how to index and what should be indexed can be found on the [RMD webpage](#).

APPENDIX K: (U) MAJOR CASES

(U) (Note: The policy for Major Cases was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

APPENDIX L: (U) ON-LINE INVESTIGATIONS

(U) (Note: The policy for On-Line Investigations was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

APPENDIX M: (U) THE FAIR CREDIT REPORTING ACT (FCRA)

(U) (Note: The policy for The Fair Credit Reporting Act was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

APPENDIX N: (U) TAX RETURN INFORMATION

(U) (Note: The policy for Tax Return Information was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

APPENDIX O: (U) RIGHT TO FINANCIAL PRIVACY ACT (RFPA)

(U) (Note: The policy for the Right to Financial Privacy Act was not completed by the time of the DIOG publication. It will be linked in the DIOG once approved.)

APPENDIX P: (U) ACRONYMS

A/EAD	Associate Executive Assistant Director
ACS	Automated Case Support
AD	Assistant Director
ADD	Associate Deputy Director
ADIC	Assistant Director-in-Charge
AFID	Alias False Identification
AG	Attorney General
AGG	Attorney General Guidelines
AGG-CHS	Attorney General Guidelines Regarding the Use of FBI Confidential Human Sources
AGG-Dom	Attorney General's Guidelines for Domestic FBI Operations
AGG-UCO	The Attorney General's Guidelines on FBI Undercover Operations
AOR	Area of Responsibility
ARS	Assessment Review Standards
ASAC	Assistant Special Agent in Charge
ASC	Assistant Section Chief
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
AUSA	Assistant United States Attorney
CALEA	Communications Assistance for Law Enforcement Act
CCRSB	Criminal Cyber Response and Services Branch

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

CD	Counterintelligence Division
CDC	Chief Division Counsel
C.F.R.	Code of Federal Regulations
CHS	Confidential Human Source
CHSPG	Confidential Human Source Policy Implementation Guide
CIA	Central Intelligence Agency
CID	Criminal Investigative Division
CMS	Collection Management Section
CPO	Corporate Policy Office
CUORC	Criminal Undercover Operations Review Committee
CyD	Cyber Division
DAD	Deputy Assistant Director
DD	Deputy Director
DEA	Drug Enforcement Administration
DGC	Deputy General Counsel
DI	Directorate of Intelligence
DLAT	Deputy Legal Attache
DNI	Director of National Intelligence
DOD	Department of Defense
DOJ	Department of Justice
DOJ OEO	Office of Enforcement Operations, DOJ

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

DOS	Department of State
DPO	Division Policy Officer
DWS-EDMS	Data Warehouse System-ELSUR Data Management System
EAD	Executive Assistant Director
EC	Electronic Communication
ECF	Electronic Case File
ECPA	Electronic Communication Privacy Act
ECS	Electronic Communication Service
EI	Enterprise Investigation
ELSUR	Electronic Surveillance
EO	Executive Order
EOT	ELSUR Operations Technician
ERS	ELSUR Records System
ESN	Electronic Serial Number
ESU	DOJ OEO, Electronic Surveillance Unit
ETR	Electronic Technical Request
FBIHQ	FBI Headquarters
FGJ	Federal Grand Jury
FGUSO	Field Guide for Undercover and Sensitive Operations
FICP	Foreign Intelligence Collection Program
FIG	Field Intelligence Group

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FLIR	Forward-looking Infrared
FRCP	Federal Rules of Criminal Procedure
GC	General Counsel
GEOINT	Geospatial Intelligence
HIPAA	Health Insurance Portability and Accountability Act
HSC	Homeland Security Council
ICE	Department of Homeland Security Immigration and Customs Enforcement
ICM	Investigative Case Management
IINI	Innocent Images National Initiative
ILB	Investigative Law Branch
ILU	Investigative Law Unit
IOB	Intelligence Oversight Board
IOD	International Operations Division
IP Address	Internet Protocol Address
IPG	Intelligence Policy Implementation Guide
ISP	Internet Service Provider
ITSMV	Interstate Transportation of Stolen Motor Vehicles
JDA	Juvenile Delinquency Act
JTTF	Joint Terrorism Task Force

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

LEGAT	Legal Attaché
LHM	Letterhead Memorandum
LO	Lead Office
MAR	Monthly Administrative Report
MLAT	Mutual Legal Assistance Treaties
MOU/MOA	Memorandum of Understanding/Agreement
MSIN	Mobile Station Identification Number
MST	Mobile Surveillance Team
MST-A	Mobile Surveillance Team—Armed
NARA	National Archives and Records Administration
NCMEC	National Center for Missing and Exploited Children
NISS	National Information Sharing Strategy
NSB	National Security Branch
NSC	National Security Council
NSD	National Security Division, DOJ
NSL	National Security Letter
NSLB	National Security Law Branch
NSSE	National Special Security Events
NSUCOPG	National Security Undercover Operations Policy Implementation Guide
OCA	Office of Congressional Affairs
OCRS	Organized Crime and Racketeering Section, DOJ

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

OGC	Office of the General Counsel
OIA	Otherwise Illegal Activity
OIC	Office of Integrity and Compliance
OIO	Office of Operations, DOJ
OLC	Office of Legal Counsel, DOJ
OO	Office of Origin
OPA	Office of Public Affairs
OTD	Operational Technology Division
PBDM	Pattern Based Data Mining
PCHS	Potential CHS
PCLU	Privacy and Civil Liberties Unit
PCTDD	Post Cut-through Dialed Digits
PFI	Positive Foreign Intelligence
PG	Policy Implementation Guide
PI	Preliminary Investigation
PIA	Privacy Impact Assessment
PIAB	President's Intelligence Advisory Board
PSA	Performance Summary Assessments
PTA	Privacy Threshold Analysis
RA	Resident Agency
RCS	Remote Computing Service

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

RF	Radio Frequency
RFPA	Right to Financial Privacy Act
RICO	Racketeer Influenced and Corrupt Organizations
RIG	Regional Intelligence Group
RMD	Records Management Division
SA	Special Agent
SAC	Special Agent-in-Charge
SC	Section Chief
SIA	Supervisory Intelligence Analyst
SIM	Sensitive Investigative Matter
SORC	Sensitive Operations Review Committee
SSA	Supervisory Special Agent
SSRA	Supervisory Senior Resident Agent
TFM	Task Force Member
TFO	Task Force Officer
TFP	Task Force Participant
TMD	Technical Management Database
TTA	Technically Trained Agent
UC	Unit Chief
UCE	Undercover Employee
UCFN	Universal Case File Number

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

UCO	Undercover Operation
UCRC	Undercover Review Committee
UDP	Undisclosed Participation
UNI	Universal Index
USA	United States Attorney
USAO	United States Attorney's Office
U.S.C.	United States Code
USG	United States Government
USIC	United States Intelligence Community
USIC	United States Intelligence Community
USIC	United States Intelligence Community
USPER	United States Person, United States Persons, US PER, USPERs, US Person, US Persons, U.S. Person, U.S. Persons
USPS	United States Postal Service
USSS	United States Secret Service
VICAP	Violent Criminal Apprehension Program
VS	Victim Services
WITT	Wireless Intercept Tracking Technology
WMD	Weapons of Mass Destruction
WMDD	Weapons of Mass Destruction Directorate

APPENDIX Q: (U) DEFINITIONS

(U//FOUO) Academic Nexus SIM: As a matter of FBI policy, an investigative activity having an “academic nexus” is considered a sensitive investigative matter (SIM) if: (i) the investigative activity involves matters related to the responsibilities of an administrator or faculty member employed by any college or university that is located inside the United States, provided the matter under a predicated investigation is related to the individual’s position at the institution; or (ii) the matter involves any student association recognized and approved by the college or university at which the student association at issue is located, and the college or university is located inside the United States. See the classified Appendix G for additional information.

(U) Aggrieved Person: A person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(U//FOUO) Assessments: The AGG-Dom authorizes as an investigative activity called an “Assessment” which requires an authorized purpose and articulated objective(s). The DIOG defines five types of Assessments that may be carried out to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence. Although “no particular factual predication” is required, the basis of an assessment cannot be arbitrary or groundless speculation, nor can an Assessment be based solely on the exercise of First Amendment protected activities or on the race, ethnicity, national origin or religion of the subject, or a combination of only those factors.

(U//FOUO) Closed Circuit Television (CCTV): a fixed-location video camera that is typically concealed from view or that is placed on or operated by a consenting party.

(U) Consensual Monitoring: Monitoring of communications for which a court order or warrant is not legally required because of the consent of a party to the communication.

(U) Electronic Communication Service: Any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, telephone companies and electronic mail companies generally act as providers of electronic communication services.

(U) Electronic Communications System: Any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(U) Electronic Storage: Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, or any storage of such communication by an electronic communication service for purposes of backup protection of such communication. In short, “electronic storage” refers only to temporary storage, made in the course of transmission, by a provider of an electronic communication service.

(U//FOUO) Electronic Tracking Device: Direction finder including electronic tracking devices, such as, radio frequency beacons and transmitters, vehicle locator units, and the various devices that use a Global Positioning System or other satellite system for monitoring non-communication activity.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Employee: For purposes of the AGG-Dom and DIOG, an “FBI employee” includes, but not limited to, an operational/administrative professional support person, intelligence analyst, special agent, task force officer (TFO), task force member (TFM), task force participant (TFP), detailee, and FBI contractor. An FBI employee is bound by the AGG-Dom and DIOG. The FBI employee definition excludes a confidential human source (CHS).

(U//FOUO) Enterprise: The term “enterprise” includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.

(U//FOUO) Enterprise Investigation: An Enterprise Investigation (EI) examines the structure, scope, and nature of the group or organization including: its relationship, if any, to a foreign power; the identity and relationship of its members, employees, or other persons who may be acting in furtherance of its objectives; its finances and resources; its geographical dimensions; its past and future activities and goals; and its capacity for harm. (AGG-Dom, Part II.C.2)

(U//FOUO) Enterprise Investigations are a type of Full Investigation and are subject to the same requirements that apply to full investigations described in Section 7. Enterprise Investigations focus on groups or organizations that may be involved in the most serious criminal or national security threats to the public, as described in Section 8. Enterprise Investigations cannot be conducted as preliminary investigations or assessments, nor may they be conducted for the sole purpose of collecting foreign intelligence. **Note:** Enterprise Investigations were designed, among other things, to combine and replace the traditional “Racketeering Enterprise Investigations” (REI) (92 classification) and “Terrorism Enterprise Investigations” (TEI) (100 classification). An EI is only authorized to be opened on the most serious criminal or national security threats. See DIOG Sections 8.4 and 8.5. The term Enterprise Investigation (EI) as used in the DIOG should not be confused with other usages of the word “enterprise,” such as criminal enterprise investigations (e.g., 281 classification, 245 classification, etc.), which are not EI’s as defined in DIOG Section 8. Although an Enterprise Investigation may not be conducted as a Preliminary Investigation, a Preliminary Investigation may be used to determine whether a group or organization is a criminal or terrorist enterprise if the FBI has “information or an allegation” that an activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur, and the investigation may obtain information relating to the activity of the group or organization in such activity. An Assessment may also be initiated to determine whether a group or organization is a criminal or terrorist enterprise.

(U//FOUO) Extraterritorial Guidelines: The guidelines for conducting investigative activities outside of the United States are currently contained in: (i) *The Attorney General’s Guidelines for Extraterritorial FBI Operations and Criminal Investigations*; (ii) *The Attorney General’s Guidelines for FBI National Security Investigations and Foreign Intelligence Collection*; and (iii) *The Attorney General Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions* (collectively, the Extraterritorial Guidelines); (iv) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (August 8, 1988); and (v) the *Memorandum of Understanding*

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation (2005).

(U//FOUO) FISA: The Foreign Intelligence Surveillance Act of 1978, as amended. The law establishes a process for obtaining judicial approval of electronic surveillance, physical searches, pen register and trap and trace devices, and access to certain business records for the purpose of collecting foreign intelligence.

(U) For or On Behalf of a Foreign Power: The determination that activities are for or on behalf of a foreign power shall be based on consideration of the extent to which the foreign power is involved in control or policy direction; financial or material support; or leadership, assignments, or discipline.

(U) Foreign Computer Intrusion: The use or attempted use of any cyber-activity or other means, by, for, or on behalf of a foreign power to scan, probe, or gain unauthorized access into one or more United States-based computers.

(U) Foreign Intelligence: Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorists.

(U) Foreign Intelligence Requirements:

- A) (U//FOUO) National intelligence requirements issued pursuant to authorization by the Director of National Intelligence, including the National Intelligence Priorities Framework and the National HUMINT Collection Directives, or any successor directives thereto;
- B) (U//FOUO) Requests to collect foreign intelligence by the President or by Intelligence Community officials designated by the President; and
- C) (U//FOUO) Directions to collect foreign intelligence by the Attorney General, the Deputy Attorney General, or an official designated by the Attorney General.

(U) Foreign Power: A foreign government or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of United States persons (USPERs); an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; a group engaged in international terrorism or activities in preparation therefore; a foreign-based political organization, not substantially composed of USPERs; or an entity that is directed or controlled by a foreign government or governments.

(U) Full Investigation: A Full Investigation may be opened if there is an “articulable factual basis” for the investigation that reasonably indicates one of the following circumstances exists:

(U) An activity constituting a federal crime or a threat to the national security has or may have occurred, is or may be occurring, or will or may occur and the investigation may obtain information relating to the activity or the involvement or role of an individual, group, or organization in such activity;

- A) (U) An individual, group, organization, entity, information, property, or activity is or may be a target of attack, victimization, acquisition, infiltration, or recruitment in connection with criminal activity in violation of federal law or a threat to the national security and the

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

investigation may obtain information that would help to protect against such activity or threat;
or

- B) (U) The investigation may obtain foreign intelligence that is responsive to a PFI requirement, as defined in DIOG Section 7.4.3.

(U) All lawful investigative methods may be used in a Full Investigation.

(U) A Full Investigation of a group or organization may be opened as an Enterprise Investigation if there is an articulable factual basis for the investigation that reasonably indicates the group or organization may have engaged, or may be engaged in, or may have or may be engaged in planning or preparation or provision of support for:

A) (U) Racketeering Activity:

- 1) (U) A pattern of racketeering activity as defined in 18 U.S.C. § 1961(5);

B) (U) International Terrorism:

- 1) (U) International terrorism, as defined in the AGG-Dom, Part VII.J, or other threat to the national security;

C) (U) Domestic Terrorism:

- 1) (U) Domestic terrorism as defined in 18 U.S.C. § 2331(5) involving a violation of federal criminal law;
- 2) (U) Furthering political or social goals wholly or in part through activities that involve force or violence and a violation of federal criminal law; or
- 3) (U) An offense described in 18 U.S.C. § 2332b(g)(5)(B) or 18 U.S.C. § 43.

(U) Human Source: A Confidential Human Source as defined in the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

(U) Intelligence Activities: Any activity conducted for intelligence purposes or to affect political or governmental processes by, for, or on behalf of a foreign power.

(U) International Terrorism: Activities that involve violent acts or acts dangerous to human life that violate federal, state, local, or tribal criminal law or would violate such law if committed within the United States or a state, local, or tribal jurisdiction; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnapping; and occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear to be intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(U//FOUO) National Security Letters: an administrative demand for documents or records that can be made by the FBI during a predicated investigation relevant to a threat to national security. The standard for issuing an NSL, except under 15 U.S.C. § 1681v, is relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person (USPER) is not predicated solely on activities protected by the First Amendment of the Constitution of the United States. Information is relevant if it tends to make a fact more or less probable. There must be a

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

reasonable belief that the information sought through the NSL either supports or weakens facts being investigated in a case.

(U//FOUO) Operational Division or Operational Unit: “Operational” division or operational unit as used in the DIOG means the FBIHQ division or unit responsible for management and program oversight of the file classification for the substantive investigative matter (i.e., Assessment or predicated investigation). Previously referred to as the FBIHQ “substantive” division or substantive unit.

(U//FOUO) Pen Register Device: Records or decodes dialing, routing addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided that such information must not include the contents of any communication.

(U//FOUO) Physical Surveillance (Not Requiring a Court Order): The deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there is no reasonable expectation of privacy. Note: DIOG Section 18.5.8 makes a distinction between “casual observation” and physical surveillance, and specifies factors to be considered when determining whether a particular plan of action constitutes casual observation or physical surveillance. (See DIOG Section 18.5.8)

(U) Preliminary Investigation: A Preliminary Investigation is a type of predicated investigation authorized under the AGG-Dom that may be opened (predicated) on the basis of any “allegation or information” indicative of possible criminal activity or threats to the national security. Preliminary Investigations may be opened to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security. However, a Preliminary Investigation cannot be opened or used solely for the purpose of collecting against Positive Foreign Intelligence (PFI) requirements or for conducting Enterprise Investigations.

(U) Proprietary: A sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship with the FBI is concealed from third parties.

(U) Provider of Electronic Communication Services: Any service that provides the user thereof the ability to send or receive wire or electronic communications.

(U) Publicly Available: Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public.

(U) Records: Any records, databases, files, indices, information systems, or other retained information.

(U) Relevance: Information is relevant if it tends to make a fact of consequence more or less probable.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U//FOUO) Remote Computing Services: The provision to the public of computer storage or processing services by means of an electronic communication system. In essence, a remote computing service is an off-site computer that stores or processes data for a customer.

(U//FOUO) Sensitive Investigative Matter: An investigative matter involving a domestic public official, domestic political candidate, religious or domestic political organization or individual prominent in such an organization, or news media, or an investigative matter having academic nexus, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBIHQ and other DOJ officials.

(U) Sensitive Monitoring Circumstance: Investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years; (Note: Executive Levels I through IV are defined in 5 U.S.C. §§ 5312-5315.)

- A) (U) Investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, concerning an offense involving bribery, conflict of interest, or extortion related to the performance of official duties;
- B) (U) A party to the communication is in the custody of the Bureau of Prisons or the United States Marshals Service or is being or has been afforded protection in the Witness Security Program; or
- C) (U) The Attorney General, the Deputy Attorney General, or an Assistant Attorney General has requested that the FBI obtain prior approval for the use of consensual monitoring in a specific investigation.

(U) Special Agent in Charge: The Special Agent in Charge of an FBI field office (including an Acting Special Agent in Charge), except that the functions authorized for Special Agents in Charge by these Guidelines may also be exercised by the Assistant Director in Charge or by any Special Agent in Charge designated by the Assistant Director in Charge in an FBI field office headed by an Assistant Director, and by FBI Headquarters officials designated by the Director of the FBI.

(U) Special Events Management: Planning and conduct of public events or activities whose character may make them attractive targets for terrorist attack.

(U) State, Local, or Tribal: Any state or territory of the United States or political subdivision thereof, the District of Columbia, or Indian tribe.

(U//FOUO) Surveillance:

- A) (U//FOUO) **Electronic surveillance (ELSUR)** - under Title III and FISA is the non-consensual electronic collection of information (usually communications) under circumstances in which the parties have a reasonable expectation of privacy and court orders or warrants are required. ELSUR is only authorized as an investigative method in the conduct of full investigations. ELSUR requires (a) administrative or judicial authorization prior to its use; (b) contact with the field office ELSUR support employee to coordinate all necessary recordkeeping; and (c) consultation with the Technical Advisor (TA) or a designated Technically Trained Agent (TTA) to determine feasibility, applicability, and use of the

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

appropriate equipment. (See DIOG Appendix Q - Definitions and Section 18 for FISA and Title III.)

- B) (U//FOUO) **Consensual monitoring of communications, including consensual computer monitoring, or electronic surveillance (ELSUR)** - where there is no reasonable expectation of privacy is permitted in Predicated Investigations. These methods usually do not require court orders or warrants unless they involve an intrusion into an area where there is a reasonable expectation of privacy or non-consensual monitoring of communications, but legal review is generally required to ensure compliance with legal requirements. Examples of this type of surveillance include, but are not limited to, CCTV, direction finders, tracking devices, etc. (See DIOG Appendix Q - Definitions and Section 18 for Consensual Monitoring, CCTV, Electronic Tracking Device, Pen Register Device, and Trap and Trace Device.)

(U//FOUO) **Physical surveillance** - is the deliberate observation by an FBI employee of persons, places, or events, on either a limited or continuous basis, in areas where there may or may not be a reasonable expectation of privacy. (See DIOG Section 18.5.8 for physical surveillance in situations not requiring a court order and a discussion of the distinction between physical surveillance and casual observation). Factors to consider in determining whether observations are casual observation or physical surveillance include: (i) the duration and frequency of the observation of a particular person or location, (ii) the location of the observation point, (iii) whether the observation is done from a stationary position or a moving position, and (iv) whether the observation is being done with the unaided eye. The use of mechanical devices operated by the user (e.g., binoculars; hand-held cameras; remotely operated and continually monitored cameras; radiation, chemical or biological detectors) is authorized provided that the device is not used to collect information in which a person has a reasonable expectation of privacy. (See also DIOG Section 18.6.3.8 (CCTV/Video Surveillance Where There is a Reasonable Expectation of Privacy in the Area to be Viewed or for the Installation of the Equipment)).

(U) **Threat to the National Security:** International terrorism; espionage and other intelligence activities, sabotage, and assassination, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General, consistent with Executive Order 12333 or a successor order.

(U//FOUO) **Trap and Trace Device:** Captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing or signaling information reasonably likely to identify the source of a wire or electronic communication, provided that such information does not include the contents of any communication.

(U//FOUO) **Undercover Activity:** An "undercover activity" is any investigative activity involving the use of an assumed identity by an undercover employee for an official purpose, investigative activity, or function.

(U//FOUO) **Undercover Employee:** An employee of the FBI, another federal, state, or local law enforcement agency, another entity of the United States Intelligence Community (USIC), or another foreign intelligence agency working under the direction and control of the FBI whose relationship with the FBI is concealed from third parties by the maintenance of a cover or alias identity for an official purpose, investigative activity, or function.

(U//FOUO) **Undercover Operation:** An "undercover operation" is an operation that involves a series of related "undercover activities" over a period of time by an "undercover employee." A

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

series of related undercover activities consists of more than five separate substantive contacts by an undercover employee with the individuals under investigation. In investigations relating to activities in violation of federal criminal law that do not concern threats to the national security or foreign intelligence, undercover activity involving sensitive circumstances, which are listed in the AGG-UCO and the FGUSO, constitutes an undercover operation regardless of the number of contacts involved. A substantive contact is a communication, whether by oral, written, wire, or electronic means, that includes information of investigative interest. Mere incidental contact (e.g., a conversation that establishes an agreed time and location for another meeting) is not a substantive contact within the meaning of this policy.

(U) United States: When used in a geographic sense, means all areas under the territorial sovereignty of the United States.

(U) United States Person (USPER): Any of the following, but not including any association or corporation that is a foreign power, defined as an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments:

- A) (U) An individual who is a United States citizen or an alien lawfully admitted for permanent residence;
- B) (U) An unincorporated association substantially composed of individuals who are United States persons (USPERs); or
- C) (U) A corporation incorporated in the United States.

(U) If a group or organization in the United States that is affiliated with a foreign-based international organization operates directly under the control of the international organization and has no independent program or activities in the United States, the membership of the entire international organization shall be considered in determining whether it is substantially composed of USPERs. If, however, the United States-based group or organization has programs or activities separate from, or in addition to, those directed by the international organization, only its membership in the United States shall be considered in determining whether it is substantially composed of USPERs. A classified directive provides further guidance concerning the determination of USPER status.

(U) Use: When used with respect to human sources, means obtaining information from, tasking, or otherwise operating such sources.

APPENDIX R: (U) SUPERCEDED DOCUMENTS AND NFIPM, MIOG, AND MAOP SECTIONS

(U//FOUO) This guide supersedes the following FBI policies and procedures:

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG Intro	Preface	Section: Preface (1)	DIOG Preamble	DIOG Preamble
MIOG Intro	Preface	Preface	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	Section: S1: Investigative Authority and Responsibility (12)	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-1 AUTHORITY OF A SPECIAL AGENT	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-2 INVESTIGATIVE RESPONSIBILITY	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 THE ATTORNEY GENERALS GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 INTRODUCTION	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3I. GENERAL PRINCIPLES	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 II. GENERAL CRIMES INVESTIGATIONS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 III. CRIMINAL INTELLIGENCE INVESTIGATIONS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 IV. INVESTIGATIVE TECHNIQUES	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 V. DISSEMINATION AND MAINTENANCE OF INFORMATION	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 VI. COUNTERTERRORISM ACTIVITIES AND OTHER AUTHORIZATIONS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-3 VII. RESERVATION	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 1	1-4 INVESTIGATIVE AUTHORITY AND THE FIRST AMENDMENT	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	Section : S2: Management and Allocation Programs (57)	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1 NATIONAL PRIORITY PROGRAMS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.1 Foreign Counterintelligence (FCI)	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.1.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.1.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.2 Organized Crime	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.2.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.2.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.2.3 Ranking of Organized Criminal Activities	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.3 Drug	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.3.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.3.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.4 Counterterrorism	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.4.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.4.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.5 White-Collar Crime	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.5.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.5.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.5.3 Ranking of Activities	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6 Violent Crimes and Major Offenders	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6.1 Fugitive Subprogram	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6.2 Government Reservation Crimes Subprogram	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6.3 Interstate Theft Subprogram	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6.4 Violent Crimes Subprogram	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-1.6.5 Violent Crimes and Major Offenders-Organized Crime Drug Enforcement Task Force Subprogram	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2 OTHER PROGRAMS	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.1.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.1.2 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.1.3 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.2 Applicant Investigations - Reimbursable and Nonreimbursable	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.2.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.2.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.2.3 Ranking of Activities	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.3 Civil Rights	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.3.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.3.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.3.3 Ranking of Activities	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.4 FBI Security Program	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.4.1 Definition	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.4.2 Objective	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.4.3 Ranking of Activities	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.5 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.5.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.5.2 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.5.3 Deleted	DIOG Preamble	DIOG Preamble

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG Intro	Section 2	2-2.6 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.6.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.6.2 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.6.3 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.7 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.7.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.7.2 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.7.3 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.8 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.8.1 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.8.2 Deleted	DIOG Preamble	DIOG Preamble
MIOG Intro	Section 2	2-2.8.3 Deleted	DIOG Preamble	DIOG Preamble
MIOG I.I	Section 7	7-5 CLARIFICATION REGARDING AN INVESTIGATION AS OPPOSED TO A PRELIMINARY INQUIRY		DIOG 5, 6 and 7
MIOG I.I	Section 7	7-6 DEPARTMENTAL INSTRUCTIONS REGARDING QUESTIONABLE CASES		Paragraphs #1 and 2 only. DIOG 5, 6 and 7
MIOG I.I	Section 7	7-20 ADMINISTRATIVE SUBPOENAS IN CHILD ABUSE AND CHILD SEXUAL EXPLOITATION (CSE) CASES		DIOG 18.6.4
MIOG I.I	Section 9	9-7.2 Use of Closed Circuit Television (CCTV)		Paragraphs #2 (all sub-parts); 3 (all sub-parts); and 4 only. DIOG 18.6.3
MIOG I.I	Section 62	62-3 DOMESTIC POLICE COOPERATION - STATUTE		
MIOG I.I	Section 62	62-3.3 Policy		Paragraphs # 5 and 6 only. DIOG 12
MIOG I.I	Section 62	62-3.4 Office of Origin		DIOG 14
MIOG I.I	Section 62	62-3.5 Classification		DIOG 12. See new 343 classification
MIOG I.2	Section 157	Section : S157 Civil Unrest (8)		DIOG 12
MIOG I.2	Section 157	157-1 RESPONSIBILITY OF THE BUREAU		DIOG 12
MIOG I.2	Section 157	157-1.1 Categories for Reporting		DIOG 12
MIOG I.2	Section 157	157-2 POLICY REGARDING REPORTING OF CIVIL DISORDERS		DIOG 12
MIOG I.2	Section 157	157-3 REPORTING OF DEMONSTRATIONS		DIOG 12
MIOG I.2	Section 157	157-4 PHOTOGRAPHIC SURVEILLANCES		DIOG 12
MIOG I.2	Section 157	157-5 DISSEMINATION OF DATA PERTAINING TO CIVIL DISORDERS AND DEMONSTRATIONS		DIOG 12
MIOG I.2	Section 157	157-6 REPORTING PROCEDURES TO BE UTILIZED IN CIVIL DISORDERS AND DEMONSTRATIONS		DIOG 12
MIOG I.2	Section 157	157-7 CHARACTER		DIOG 12
MIOG I.2	Section 161	161-10 DISSEMINATION TO THE WHITE HOUSE COMPLEX (WHC)		DIOG 14, 18
MIOG I.2	Section 163	163-1.1 Investigative Request		DIOG 12
MIOG I.2	Section 163	163-2 INVESTIGATIVE INSTRUCTIONS AND PROCEDURES		DIOG 12
MIOG I.2	Section 163	163-2.1 Opening Foreign Police Cooperation (FPC) - General Criminal Matters (GCM)		In-part, Paragraphs #1 a and b; #2; and #6 only for new 163 classifications. DIOG 12
MIOG I.2	Section 163	163-2.1.1 Letter Rogatory Process		DIOG 12
MIOG I.2	Section 163	163-3 REQUESTS FOR TERRORISM ENTERPRISE INVESTIGATIONS		DIOG 8 and 12
MIOG I.2	Section 163	163-6 REPORTING		DIOG 12
MIOG I.2	Section 163	163-7 RULE 6(E) MATERIAL		DIOG 18
MIOG I.2	Section 163	163-8 PRIVACY ACT		DIOG 14
MIOG I.2	Section 163	163-9 RIGHT TO FINANCIAL PRIVACY ACT		DIOG Appendix O
MIOG I.2	Section 288	288-5.1 Accessing Computer Records - Summary of Compelled Disclosure under Title 18, USC, Section 2703		DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.1 Subpoena - ECPA Requirements		DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.2 Subpoena with Prior Notice to the Subscriber or Customer		DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.3 Section 2703(d) Order		DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.4 Section 2703(d) Order with Prior Notice to the Subscriber or Customer		DIOG 18.6.8
MIOG I.2	Section 288	288-5.1.5 Search Warrant		DIOG 18.7.1
MIOG I.2	Section 288	288-5.1.6 Voluntary Disclosure		DIOG 18.6.8
MIOG I.2	Section 289	289-13.3 Use of a Past or Present Prisoner-Witness in an Investigation (Formerly Part 2, 27-16.5)	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG I.2	Section 308	308-1.1 Evidence Response Team Mission		generally, DIOG 12 for expert assistance.
MIOG I.2	Section 308	308-2 DEFINITION OF ERT CONCEPT		Paragraph # 4 only. DIOG 12
MIOG I.2	Section 308	308-3 PROPER TURNING		Paragraph # 2 only. DIOG 12

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG I.2	Section 308	308-4 ERT SUBCLASSIFICATIONS-ALPHA DESIGNATORS		Paragraph # 1 only. DIOG 12. See new classifications
MIOG I.2	Section 319	319-1 INTELLIGENCE PROGRAM		generally, DIOG 5
MIOG I.2	Section 319	319-2 FIELD INTELLIGENCE GROUP (FIG) STRUCTURE AND FUNCTIONS		generally, DIOG 5
MIOG I.2	Section 319	319-4 INTELLIGENCE COLLECTION		Paragraphs # 1 and 3 generally, DIOG 5 generally, DIOG 5
MIOG I.2	Section 319	319-5 COLLECTION MANAGEMENT		
MIOG II	Section 2	2-5 COMPLAINTS (RULE 3)		DIOG 19
MIOG II	Section 2	2-5.1 Authorization of U.S. Attorney (USA)		DIOG 19
MIOG II	Section 2	2-5.3 State Prosecutions		DIOG 3, 12
MIOG II	Section 2	2-5.4 Authority for Issuance of Warrant		DIOG 19
MIOG II	Section 2	2-5.5 Notification to Special Agent in Charge (SAC)		DIOG 19
MIOG II	Section 2	2-6 WARRANT OF ARREST OR SUMMONS (RULE 4)		DIOG 18 and 19
MIOG II	Section 2	2-6.1 Forms of Warrant		DIOG 19
MIOG II	Section 2	2-6.2 Issuance of Warrant or Summons		DIOG 19
MIOG II	Section 2	2-6.3 Execution		DIOG 19
MIOG II	Section 2	2-7 PROCEEDINGS BEFORE THE MAGISTRATE (RULE 5)		DIOG 18 and 19
MIOG II	Section 2	2-7.1 Initial Appearance		DIOG 19
MIOG II	Section 2	2-9 GRAND JURY (RULE 6)	DIOG 11.9 – 11.9.1	DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.1 Purpose		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.2 Persons Present		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.3 Disclosure		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.4 Exceptions	DIOG 11.9 – 11.9.1	DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.5 Limitation of Use		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.5.1 Matters Occurring Before the Grand Jury	DIOG 11.9 – 11.9.1	DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.5.2 Physical Evidence and Statements		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.6 Documentation of Disclosures of Grand Jury Material		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.6.1 Documentation of Internal Disclosures of Grand Jury Material		DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.7 Storage of Grand Jury Material	DIOG 11.9 – 11.9.1	DIOG 18.5.9 and 18.6.5
MIOG II	Section 2	2-9.8 Requests for Subpoenas in Fugitive Investigations	DIOG 11.9 – 11.9.1	DIOG 18.5.9 and 18.6.5
MIOG II	Section 4	S4 Juveniles and Juvenile Delinquency Act		DIOG 19
MIOG II	Section 4	4-1 GENERAL STATEMENT		DIOG 19
MIOG II	Section 4	4-1.1 Purpose of Act		DIOG 19
MIOG II	Section 4	4-2 SPECIFIC PROVISIONS OF THE ACT		DIOG 19
MIOG II	Section 4	4-2.1 Definitions		DIOG 19
MIOG II	Section 4	4-2.2 Arrest Procedure		DIOG 19
MIOG II	Section 4	4-2.2.1 Advice of Rights		DIOG 19
MIOG II	Section 4	4-2.2.2 Notification of USA and Juveniles Parents		DIOG 19
MIOG II	Section 4	4-2.2.3 Fingerprinting and Photographing		DIOG 19
MIOG II	Section 4	4-2.2.4 Press Releases		DIOG 19
MIOG II	Section 4	4-2.2.5 Interviews of Juveniles		DIOG 18
MIOG II	Section 4	4-2.2.6 Initial Appearance Before Magistrate		DIOG 19
MIOG II	Section 4	4-2.3 Detention		DIOG 19
MIOG II	Section 4	4-2.4 Prosecution		DIOG 19
MIOG II	Section 4	4-2.5 Use of Juvenile Records		DIOG 19
MIOG II	Section 7	S7 Interviews		DIOG 18.5.6
MIOG II	Section 7	7-1 USE OF CREDENTIALS FOR IDENTIFICATION		DIOG 18.5.6
MIOG II	Section 7	7-2 THOROUGHNESS, PRECAUTIONS, TELEPHONIC AND USE OF INTERPRETERS		DIOG 18.5.6
MIOG II	Section 7	7-2.1 Thoroughness and Precautions During Interviews		DIOG 18.5.6
MIOG II	Section 7	7-2.2 Telephone Interviews		DIOG 18.5.6
MIOG II	Section 7	7-2.3 Use of Interpreters		DIOG 18.5.6
MIOG II	Section 7	7-3 REQUIRING FBIHQ AUTHORITY		DIOG 18.5.6
MIOG II	Section 7	7-4 ONE VS TWO AGENT INTERVIEW OF SECURITY SUBJECT		DIOG 18.5.6
MIOG II	Section 7	7-5 EVALUATION OF AN INTERVIEW		DIOG 18.5.6
MIOG II	Section 7	7-6 INTERVIEWING COMPLAINANTS AND SUBJECTS OF CRIMINAL		DIOG 18.5.6
MIOG II	Section 7	7-6.1 Interviews of Complainants		DIOG 18.5.6
MIOG II	Section 7	7-6.2 Subjects of Criminal Investigations		DIOG 18.5.6
MIOG II	Section 7	7-7 DEVELOPMENT OF DEROGATORY INFORMATION DURING INTERVIEWS		DIOG 18.5.6
MIOG II	Section 7	7-8 IDENTIFICATION OF SUSPECTS		DIOG 18.5.6
MIOG II	Section 7	7-9 INTERVIEWS INVOLVING OR RELATING TO COMPLAINTS		DIOG 18.5.6 and 5

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG II	Section 7	7-9.1 Complaints Received at the Field Office		DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.2 Complaints in Person or by Telephone		DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.3 Complaints By Letter		DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.4 Complaints Critical of the FBI or Its Employees		DIOG 18.5.6 and 5
MIOG II	Section 7	7-9.5 Legal Requirements of the Privacy Act of 1974 (Title 5, USC, Section 552a)		DIOG 14
MIOG II	Section 9	S9 Surveillances		DIOG 18.5.8
MIOG II	Section 9	9-1 GENERAL GUIDELINES		DIOG 18.5.8
MIOG II	Section 9	9-1.1 Surveillance Restrictions		DIOG 18
MIOG II	Section 9	9-7.5 Surveillance Logs		DIOG 3
MIOG II	Section 10	S10 Records Available and Investigative Techniques		DIOG 18
MIOG II	Section 10	10-1 INTRODUCTION		DIOG 18
MIOG II	Section 10	10-2 RECORDS AVAILABLE		DIOG 18
MIOG II	Section 10	10-3 INVESTIGATIVE TECHNIQUES		In-part DIOG 18
MIOG II	Section 10	10-6 MAIL COVERS		DIOG 18.6.10
MIOG II	Section 10	10-6.1 United States Postal Service (USPS) Regulations		DIOG 18.6.10
MIOG II	Section 10	10-6.2 Policy	DIOG 11.3	DIOG 18.6.10
MIOG II	Section 10	10-6.3 Requesting Approval	DIOG 11.3	DIOG 18.6.10
MIOG II	Section 10	10-6.3.1 Fugitive or Criminal Cases		DIOG 18.6.10
MIOG II	Section 10	10-6.3.2 National Security Cases		DIOG 18.6.10
MIOG II	Section 10	10-7 STOP NOTICES		DIOG
MIOG II	Section 10	10-7.1 Definition		DIOG
MIOG II	Section 10	10-7.2 Placement of Stops		DIOG
MIOG II	Section 10	10-7.3 Indexing Stops		DIOG
MIOG II	Section 10	10-7.4 Removal of Stops		DIOG
MIOG II	Section 10	10-7.5 Types of Stops		DIOG
MIOG II	Section 10	10-7.5.1 Savings Bonds		DIOG
MIOG II	Section 10	10-7.5.2 Immigration and Naturalization Service (INS)		DIOG
MIOG II	Section 10	10-7.5.3 Bureau of Prisons		DIOG
MIOG II	Section 10	10-8 STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS		DIOG 18.6.8
MIOG II	Section 10	10-8.1 Compelled Disclosure of the Contents of Stored Wire or Electronic Communications	DIOG 11.12	DIOG 18.6.8
MIOG II	Section 10	10-8.2 Access to Transactional Information		DIOG 18.6.8
MIOG II	Section 10	10-8.3 Access to and Use of Electronic Communications Located on the Internet, E-Mail, and Bulletin Board Systems		DIOG 18.6.8
MIOG II	Section 10	10-8.3.1 Definitions		DIOG 18.6.8
MIOG II	Section 10	10-8.3.2 Interception of Electronic Communications	DIOG 11.12	DIOG 18.6.8
MIOG II	Section 10	10-8.3.3 Undercover Use of the Internet		DIOG 18.6.8
MIOG II	Section 10	10-8.4 Monitoring the Internet		DIOG 18.6.8
MIOG II	Section 10	10-9 ELECTRONIC SURVEILLANCE (ELSUR) PROCEDURES AND REQUIREMENTS	DIOG 11.12	DIOG 18.7.2
MIOG II	Section 10	10-9.1 Definitions	DIOG 11.6.4,5	DIOG 18.7.2
MIOG II	Section 10	10-9.4 ELSUR Searching Procedures	DIOG 11.6.6	DIOG 18.7.2
MIOG II	Section 10	10-9.10 Electronic Surveillance - Title III Criminal Matters	DIOG 11.12	DIOG 18.7.2
MIOG II	Section 10	10-9.11 Emergency Provisions, Title III Criminal Matters		DIOG 18.7.2 and 05/22/2008 memo
MIOG II	Section 10	10-9.11.1 Form 2 Report		DIOG 18
MIOG II	Section 10	10-9.11.2 Completion of Form 2 Report		DIOG 18
MIOG II	Section 10	10-9.11.3 Submissions of Form 2 Report to FBIHQ		DIOG 18
MIOG II	Section 10	10-9.11.4 Supplemental Form 2 Reports		DIOG 18
MIOG II	Section 10	10-9.12 ELSUR Indexing in Title III Criminal Matters		DIOG 18
MIOG II	Section 10	10-9.13 Marking of Recordings for Identification		DIOG 18
MIOG II	Section 10	10-9.14 Loan of Electronic Surveillance Equipment to State and Local Law Enforcement Agencies		DIOG 12
MIOG II	Section 10	10-9.15 Submission of Recordings		DIOG 18
MIOG II	Section 10	10-9.16 Transcription of Recordings		DIOG 18
MIOG II	Section 10	10-10 CONSENSUAL MONITORING - CRIMINAL MATTERS		DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.1 Use of Consensual Monitoring in Criminal Matters	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.2 Monitoring Telephone Conversations in Criminal Matters	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.2.1 Access to Recordings and Information Concerning Monitored Inmate Telephone Calls in Federal Prisons	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.3 Monitoring Nontelephone Communications in Criminal Matters	DIOG 11.5	DIOG 18.6.1 and 18.6.2

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG II	Section 10	10-10.4 Monitoring Communications with Persons Outside the United States	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.5 ELSUR Indexing in Consensual Monitoring Matters	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.5.1 Administration of ELSUR Records Regarding Informants and Assets	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.6 Use of Consensual Monitoring in National Security Matters	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 10	10-10.7 Pen Registers (Dialed Number Recorder)	DIOG 11.11	DIOG 18.6.9
MIOG II	Section 10	10-10.7.1 Emergency Provisions		DIOG 18.6.9
MIOG II	Section 10	10-10.8 Electronic Tracking Devices	DIOG 11.6.3	DIOG 18.7.2
MIOG II	Section 10	10-10.9 Closed Circuit Television (CCTV) (Video Only) - Criminal Matters		DIOG 18.6.3
MIOG II	Section 10	10-10.9.1 CCTV Authorization - Criminal Matters		DIOG 18.6.3.4-5
MIOG II	Section 10	10-10.9.2 CCTV - ELSUR Records - Criminal Matters		DIOG 18.6.3
MIOG II	Section 10	10-10.9.3 CCTV (Audio and Video) - ELSUR Indexing - Criminal Matters		DIOG 18.6.3
MIOG II	Section 10	10-10.9.4 CCTV - Preservation of the Original Tape Recording		DIOG 18.6.3.7
MIOG II	Section 10	10-10.10 Media Recorders (Formerly Tape Recorders)		DIOG 18.6.1
MIOG II	Section 10	10-10.11 Radio Monitoring		DIOG 18.6.1
MIOG II	Section 10	10-10.11.1 Paging Devices		DIOG 18.6.1
MIOG II	Section 10	10-10.11.2 Cordless Telephones and Other Types of Radio Monitoring		DIOG 18.6.1
MIOG II	Section 10	10-10.11.3 Cellular Telephones		DIOG 18.6.1
MIOG II	Section 10	10-10.17 Trap-Trace Procedures	DIOG 11.11	DIOG 18.6.9
MIOG II	Section 10	10-10.17.1 Emergency Provisions		DIOG 18.6.9
MIOG II	Section 10	10-11 FBI UNDERCOVER ACTIVITIES - CRIMINAL MATTERS		DIOG 18.6.13
MIOG II	Section 10	10-18 FBI PRINCIPLES AND POLICIES FOR ONLINE CRIMINAL INVESTIGATIONS		DIOG Appendix L
MIOG II	Section 10	10-18.1 Online Communications		DIOG Appendix L
MIOG II	Section 10	10-18.2 Monitoring Online Communications		DIOG Appendix L
MIOG II	Section 10	10-18.3 Access to Stored Electronic Information		DIOG Appendix L
MIOG II	Section 10	10-18.4 Record Retention and Dissemination		DIOG 14 and Appendix L
MIOG II	Section 10	10-18.5 Undercover Online Communications		DIOG Appendix L
MIOG II	Section 10	10-18.6 International Issues		DIOG Appendix L
MIOG II	Section 10	10-19 HANDLING AND PRESERVATION OF AIRCRAFT-MOUNTED VIDEO AND FORWARD-LOOKING INFRARED (FLIR) EVIDENCE	DIOG 11.6.6	DIOG 18.6.3.6
MIOG II	Section 10	10-20 MAJOR CASES		DIOG Appendix K - Major cases
MIOG II	Section 11	S11 Techniques and Mechanics of Arrest		DIOG 19
MIOG II	Section 11	11-1 ARREST TECHNIQUES		DIOG 19
MIOG II	Section 11	11-1.1 General		DIOG 19
MIOG II	Section 11	11-1.2 Initial Approach		DIOG 19
MIOG II	Section 11	11-1.3 Search of the Person		DIOG 19
MIOG II	Section 11	11-1.3.1 High-Risk Search-Full-Body Search-Handcuffing		DIOG 19
MIOG II	Section 11	11-1.3.2 Final Search and Collection of Evidence		DIOG 19
MIOG II	Section 11	11-1.4 Transportation of Arrested Persons		DIOG 19
MIOG II	Section 11	11-1.5 Handcuffing		DIOG 19
MIOG II	Section 11	11-2 PROCEDURES FOR ARREST		DIOG 19
MIOG II	Section 11	11-2.1 Arrests and Searches		DIOG 19
MIOG II	Section 11	11-2.1.1 Types of Arrest Warrants		DIOG 19
MIOG II	Section 11	11-2.1.2 Authority to Serve Arrest Warrants		DIOG 19
MIOG II	Section 11	11-2.1.3 Summons and Subpoenas		DIOG 18
MIOG II	Section 11	11-2.1.4 Arrests Without Warrants		DIOG 19
MIOG II	Section 11	11-2.1.5 Forcible Entry		DIOG 19
MIOG II	Section 11	11-2.1.6 Search of the Person		DIOG 19
MIOG II	Section 11	11-2.2.2 Property of Prisoner		DIOG 19
MIOG II	Section 11	11-2.2.3 Removal of Prisoner from the Custody of the U.S. Marshal		DIOG 19
MIOG II	Section 11	11-2.3.2 Medical Attention for Bureau Subjects		DIOG 19
MIOG II	Section 11	11-2.3.3 Arrest of Foreign Nationals		DIOG 19
MIOG II	Section 11	11-4.7.1 Juveniles		DIOG 19
MIOG II	Section 12	12-2.1 Deadly Force - Standards for Decisions		DIOG has pdf of policy in Appendix F
MIOG II	Section 14	14-16.9 Fingerprinting of Juveniles by Federal Agencies under the Violent Crime Control and Law Enforcement Act of 1994 (Hereinafter, the Act)		DIOG 19

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIOG II	Section 16	16-4.1.2 Dialed Number Recorders (Pen Registers)		Paragraph #1, last two sentences only. DIOG 18.6.9
MIOG II	Section 16	16-4.1.3 Consensual Monitoring (Formerly 16-7.4.1)		Paragraphs # 3 and 4 only. DIOG 18.6.1
MIOG II	Section 16	16-4.1.4 Electronic Surveillance - Title III		DIOG 18.7.2
MIOG II	Section 16	16-4.1.5 Electronic Surveillance FISA		DIOG 18.7.3
MIOG II	Section 16	16-4.1.6 Telephone Toll Records		DIOG 18
MIOG II	Section 16	16-4.2.2 Court-Ordered Electronic Surveillance (RCU)		DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.3 Computing Time for Title III Electronic Surveillance (RCU)		DIOG 18.7.2
MIOG II	Section 16	16-4.2.4 Emergency Electronic Surveillance (RCU)		DIOG 18.6.9; 18.7.2; and 18.7.3
MIOG II	Section 16	16-4.2.5 Roving Electronic Surveillance (RCU)		DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.3 Consensual Monitoring - Technical Assistance (RCU)		Paragraph # 1, first two sentences only. DIOG 18.6.1 and 18.6.2
MIOG II	Section 16	16-4.4 Electronic Surveillance (ELSUR) Interceptions (RCU)		Paragraph # 1, first sentence only. DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.2 Telecommunications Interceptions - Reporting Requirements (TICTU)		DIOG 18.7.2 and 18.7.3
MIOG II	Section 16	16-4.4.3 Telecommunications - Use of Pen Registers and Traps-Traces (TICTU)		Paragraph # 1 only. DIOG 18.6.9
MIOG II	Section 16	16-4.4.4 Pen Registers and Traps-Traces Reporting Requirements (TICTU)		DIOG 18.6.9
MIOG II	Section 16	16-4.8.1 Authorized Use of Technical Devices in Conducting Physical Surveillances (TTU)		Paragraph # 1, second, third and fourth sentences only. DIOG 18
MIOG II	Section 16	16-4.8.4 Technical Devices in Physical Surveillance - Technical, Practical, and Legal Considerations (TTU)		Paragraph # 1 only. DIOG 18
MIOG II	Section 16	16-4.8.9 Authorized Use of Electronic Tracking and Locating Devices and Techniques (TTU)		DIOG 18
MIOG II	Section 16	16-4.8.12 Tracking - Technical, Practical, and Legal Considerations (TTU)		Paragraph # 1; Paragraph # 2, third sentence; Paragraph # 4, second sentence only. DIOG 18
MIOG II	Section 16	16-4.9 Closed Circuit Television (CCTV) (VSU)		DIOG 18.6.3
MIOG II	Section 16	16-4.13.1 Availability and Control of Technical Equipment		Paragraphs # 2 and 3 only. DIOG 18
MIOG II	Section 16	16-4.13.4 Loan of Electronic Surveillance Equipment		DIOG 12
MIOG II	Section 21	21-12 APPREHENSION OF BUREAU FUGITIVES		Paragraph # 1 only. DIOG 19
MIOG II	Section 21	21-13.4 Policy		Paragraphs # 2 and 3 only. DIOG 19
MIOG II	Section 21	21-20 FUGITIVE INVESTIGATIONS FOR OTHER FEDERAL AGENCIES		Paragraph # 3, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 21	21-20.1 Fugitive Inquiries Abroad on Behalf of U.S. Marshals Service (USMS)		Paragraph # 4, new classification 343 replaces 62. DIOG 12.5
MIOG II	Section 23	23-2 THE FAIR CREDIT REPORTING ACT		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.1 Section 1681a. Definitions		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.2 Section 1681b. Permissible Purposes of Consumer Reports		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.3 Section 1681f. Disclosures to Government Agencies		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.4 Section 1681g. Disclosure to Consumers		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.5 Section 1681e. Compliance Procedures		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.6 Summary		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.7 Penalties		DIOG Appendix M - FCRA
MIOG II	Section 23	23-2.8 Section 1681n, o, q, and r. Civil and Criminal Liability for Willful or Negligent Noncompliance		DIOG Appendix M - FCRA
MIOG II	Section 23	23-4.4 Interviews in Foreign Countries		DIOG 18
MIOG II	Section 23	23-4.10 Extraterritorial Investigative Activity	DIOG 11.5	DIOG 18.6.1 and 18.6.2
MIOG II	Section 23	23-6 TITLE XI, RIGHT TO FINANCIAL PRIVACY ACT OF 1978 (RFPA)		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.1 Statute		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2 Access to Financial Records		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.1 Intent		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.2 Methods Available to FBI		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.2.3 Methods Not Available to FBI		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3 Definitions		DIOG Appendix O - RFPA
MIOG II	Section 23	23-6.3.1 Financial Institution		DIOG Appendix O - RFPA

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MIQG II	Section 23	23-6.3.2 Financial Record		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.3.3 Government Authority		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.3.4 Customers Covered		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.3.5 Law Enforcement Inquiry		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.4 Responsibility of Financial Institutions		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.5 Certification of Compliance		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6 Methods of Access		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6.1 Customer Authorization		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6.2 Search Warrants		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6.3 Formal Written Request		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6.4 Judicial Subpoena		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.6.5 Grand Jury Subpoena		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.7 Customer Notice		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.7.1 Contents of Notice		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.7.2 Delay of Notice		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.8 Customer Challenges		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.9 Emergency Access		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10 Exceptions to RFPa		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.1 Financial Institutions		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.2 Corporations or Other Legal Entities		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.3 Not Identifiable with Customer		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.4 Parties in Interest		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.5 Federal Grand Jury		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.6 Foreign Counterintelligence		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.7 Telephone Company Toll Records		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.10.8 Other		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.11 Dissemination of Information		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.11.1 To Department of Justice		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.11.2 To Other Departments		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.12 Penalties		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.12.1 Civil		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.12.2 Disciplinary Action		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.12.3 Other		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.13 Cost Reimbursement		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.14 Reporting Requirements		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.14.1 Dissemination of Information Obtained		DIOG Appendix O - RFPa
MIQG II	Section 23	23-6.14.2 Statistical Reporting		DIOG Appendix O - RFPa
MIQG II	Section 28	28-1 ATTORNEY GENERAL'S GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES		DIOG Appendix C
NFIPM	Section 1	01-2: (U) The National Security List		DIOG Appendix G
NFIPM	Section 1	01-3: (U) Acronyms		DIOG Appendix P
NFIPM	Section 1	01-4: (U) File Classifications and Alpha Designations for Investigative and Administrative Activities Which Uniquely Fall Within the Purview of the FBI's National Foreign Intelligence Program		CPD #0015D: See RPO web-page.
NFIPM	Section 2	02-1: (U) General Investigative and Administrative Activities		Appendix M for definitions: #2, 6, 7, 10, 12, 14, 15, 18, 19, 20, 25, 26 and 27.
NFIPM	Section 2	02-2: (U) National Security Investigations		DIOG 5, 6, 7, 8, 9
NFIPM	Section 2	02-3: (U) Summary Guidance and Applicability of Threat Assessments		DIOG 5
NFIPM	Section 2	02-4: (U) Summary Guidance and Applications for Preliminary Investigations		DIOG 6 and 18
NFIPM	Section 2	02-5: (U) Summary Guidance and Application for Full Investigations (FI)		DIOG 7, 8, 9 and 18
NFIPM	Section 2	02-6: (U) Collection of Foreign Intelligence		DIOG 9
NFIPM	Section 2	02-8: (U) Office of Origin		DIOG 14
NFIPM	Section 2	02-9: (U) Physical and Photographic Surveillances		DIOG 18.5.8
NFIPM	Section 2	02-10: (U) Interviews in National Security Investigations		DIOG 18.5.6
NFIPM	Section 2	02-11: (U) Education Records (Buckley Amendment)		DIOG Appendix I
NFIPM	Section 2	02-12: (U) Polygraph Examinations		DIOG 18.6.11
NFIPM	Section 2	02-14: (U) CIA Name Searches		DIOG 19.2 and Appendix G
NFIPM	Section 2	02-15: (U) Physical Searches in Which a Warrant is Not Required	DIOG 11.4	DIOG 18.6.12
NFIPM	Section 2	02-16: (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy		DIOG 18.6.3
NFIPM	Section 2	02-17: (U) National Security Letters (NSL)	DIOG 11.9-11.9.3	DIOG 18.6.6

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
NFIPM	Section 2	02-19: (U) Business Records		DIOG 18.6.7
NFIPM	Section 2	02-21: (U) Mail Covers	DIOG 11.3	DIOG 18.6.10
NFIPM	Section 2	02-22: (U) Operations Conducted Outside the United States, the CIA MOU		See CPO MOU Library
NFIPM	Section 2	02-23: (U) The Role of Legal Attaches in Foreign Counterintelligence, Foreign Intelligence and Counterterrorism Investigations		See IOD PG
NFIPM	Section 2	02-24: (U) Otherwise Illegal Activities		DIOG 17.
NFIPM	Section 2	02-25: (U) Arrests, Interdictions, Demarches and Declarations		DIOG 19 - Arrest Procedure
NFIPM	Section 2	02-29: (U) Laboratory Assistance		See Lab web-page
NFIPM	Section 2	02-32: (U) Blind Faith Program		DIOG 19.3, 19.4 and appendix G - 12.C
NFIPM	Section 2	02-33: (U) Foreign Counterintelligence and Counterterrorism Lookout (LO) Program		DIOG Appendix G - 12.C
NFIPM	Section 2	02-34: (U) Special Surveillance Group (SSG) Program		DIOG 18.5.8
NFIPM	Section 2	02-35: (U) The Behavioral Analysis Program (BAP)		DIOG 19.4
NFIPM	Section 2	02-36: (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad		DIOG 10, generally
NFIPM	Section 2	02-37: (U) Investigations of Current and Former Central Intelligence Agency Personnel		DIOG 10, generally
NFIPM	Section 2	02-38: (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel		DIOG 10, generally
NFIPM	Section 2	02-39: (U) Investigations of Current and Former Department of Energy Personnel		DIOG 10, generally
NFIPM	Section 2	02-40: (U) Investigations of Other Government Agency Personnel		DIOG 10
NFIPM	Section 2	02-41: (U) Investigations of White House Personnel		DIOG 10
NFIPM	Section 2	02-42: (U) Investigations of Presidential Appointees		DIOG 10
NFIPM	Section 2	02-43: (U) Investigations of Members of the Judiciary		DIOG 10
NFIPM	Section 2	02-44: (U) Investigations of Members of the U.S. Congress and their Staffs		DIOG 10
NFIPM	Section 2	02-45: (U) Disseminating Information to Other Agencies in the Federal Government		DIOG 12.4/DIOG 14
NFIPM	Section 2	02-47: (U) Disseminating Information to Congressional Committees		DIOG 12.4 and 14.3(A)(4)
NFIPM	Section 2	02-48: (U) Disseminating Information to the Federal Judiciary		DIOG 12.4
NFIPM	Section 2	02-49: (U) Disseminating Information to the White House		DIOG 12.4 and 14.5
NFIPM	Section 2	02-50: (U) Disseminating Information to Foreign Governments and Investigations at their Behest		DIOG 12.4/DIOG 14.5
NFIPM	Section 2	02-51: (U) Disseminating Information to State and Local Government Agencies		DIOG 12 and 14
NFIPM	Section 2	02-52: (U) Disseminating Information to the Private Sector		DIOG 14.3 (A)(6-8)
NFIPM	Section 2	02-54: (U) IIIA (Integrated Intelligence Information Application)		See IIIA web-page
NFIPM	Section 2	02-56: (U) Intelligence Oversight Board Matters		DIOG 4/DIOG 18.6.6 (Re: NSLs) and CPD 0188PG
NFIPM	Section 2	02-57: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 3	03-1: (U) Consensual Monitoring	DIOG 11.5	DIOG 18.6.1
NFIPM	Section 3	03-2: (U) Volunteered Tape Recordings	DIOG 6.9(B)(7)	DIOG 18.5.7
NFIPM	Section 3	03-4: (U) Pen Registers and Trap and Trace Devices	DIOG 11.11-11.12	DIOG 18.6.9
NFIPM	Section 3	03-5: (U) Unconsented Electronic Surveillance	DIOG 11.12	DIOG 18.7.3
NFIPM	Section 3	03-6: (U) Electronic Surveillance Minimization, Logs and Indexing		0137PG
NFIPM	Section 3	03-8: (U) Operational Support to the Intelligence Community	DIOG 12.5/DIOG 14.5	DIOG 12
NFIPM	Section 3	03-9: (U) Operational Technology Division (OTD) Technical Assistance		CPD #0170D
NFIPM	Section 3	Section 3-10 (U) Operational Technology Division (OTD) Technical Assistance Support to the Intelligence Community		DIOG 12 (generally)
NFIPM	Section 3	03-11: (U) Unconsented Physical Searches	DIOG 11.13	DIOG 18.7.1
NFIPM	Section 3	03-12: (U) Tax Return Information		Appendix N - Tax Return Info
NFIPM	Section 3	03-13: (U) Searches of Mail Without Consent		DIOG 18.7.1
NFIPM	Section 3	03-14: (U) Unconsented Physical Search Minimization, Logs and Indexing		DIOG 18.7.1 and SMP PG
NFIPM	Section 4	04-1: (U) The Domain Program		DIOG 5, type 4 assessments generally.
NFIPM	Section 5	05-2: (U) Countries on the Current National Security List		Appendix G

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
NFIPM	Section 5	05-23: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 6	06-12: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 8	08-11: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 9	09-8: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 11	11-4: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 12	12-4: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 13	13-4: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 14	14-4: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 15	15-4: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 16	16-13: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 18	18-3: (U) Issue Threat Preliminary Investigations		DIOG 6
NFIPM	Section 18	18-4: (U) Issue Threat Full Investigations		DIOG 7
NFIPM	Section 18	18-6: (U) Issue Threat File Numbers		CPD #0015D. See RPO web-page.
NFIPM	Section 19	19-3: (U) Procedural Requirements in International Terrorism Investigations		DIOG 5, 6, 7, 8
NFIPM	Section 19	19-4: (U) Closing International Terrorism Investigations	DIOG 5,6,7	DIOG 5, 6, 7, 8
NFIPM	Section 19	19-11: (U) The Behavioral Analysis Program		DIOG 19.4
NFIPM	Section 19	19-13: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 20	20-9 (U) The Behavioral Analysis Program		DIOG 19.4
NFIPM	Section 20	20-10 (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 21	21-6: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 22	22-2: (U) Alpha Designations		CPD #0015D. See RPO web-page.
NFIPM	Section 27	Confidential Human Sources Manual		CHSPM
NFIPM	Section 27	Confidential Human Source Validation Standards Manual		CSHVSM
NFIPM	Section 28	Section : 28 (U) Undercover Operations (4)		DIOG and NSUCOPG
NFIPM	Section 28	28-1: (U) UC Operations	DIOG 11.12	DIOG 18.6.3 and NSUCOPG
NFIPM	Section 28	28-2: (U) Group I	DIOG 11.12	DIOG 18.6.3 and NSUCOPG
NFIPM	Section 28	28-3: (U) Group II	DIOG 11.12	DIOG 18.6.3 and NSUCOPG
NFIPM	Section 28	28-4: (U) UC Administrative Matters	DIOG 11.12	DIOG 18.6.3 and NSUCOPG
NFIPM	Section 30	30-11: (U) The Behavioral Analysis Program Appendix T		DIOG 19.4
	MAP T	Memorandum of Understanding between the National Aeronautics and Space Administration and the FBI		CPO MOU Library
MAOP I	0-1	Authority of the Director		DIOG 3.2.1
MAOP I	21-7 (6)	Monitoring, documenting and reviewing		DIOG 3.4.D
MAOP II	1-1	SAC and ASAC Supervisory Responsibility		Paragraphs # 2 and # 5. DIOG 3.4.C and Succession and delegation policy
MAOP II	1-1.4 (# 1)	Supervision of Cases		Paragraph # 1 - DIOG 14
MAOP II	1-1.4 (# 2 and # 3 a-f)	Supervisory File Reviews		Paragraph # 2 and # 3 (a-f) - # 2 Supervisory File reviews and # 3 PSAs. DIOG 3.4.D
MAOP II	1-1.5.1	Official Channels		Paragraph (5) b only - superseded by CPD 0152D - FBI Policy Cycle Directive.
MAOP II	1-3.5	Designation of Senior Resident Agent and Alternate		Second and third sentences only - DIOG 3.4.C and succession and delegation policy ?
MAOP II	1-3.6	Reporting to HQ City		First and second sentence - file reviews every 90 days: DIOG 3.4.D

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MAOP II	1-3.13.2 (1)	Supervision of Investigations		Paragraph (1) - DIOG 3.4.C and succession and delegation policy ?
MAOP II	1-3.13.3 (all)	Case Reviews		All (paragraphs 1-6) - DIOG 3.4.D
MAOP II	2-3	Indexing		DIOG 14
MAOP II	2-3.1	Purpose		DIOG 14
MAOP II	2-3.2	General Policy		DIOG 14
MAOP II	2-3.3	Indexing Criteria and Guidelines		DIOG 14
MAOP II	2-3.3.1	Mandatory Indexing		DIOG 14
MAOP II	2-3.3.2	Discretionary Indexing		DIOG 14
MAOP II	2-3.4	Index Data		DIOG 14
MAOP II	2-3.4.1	Identifying Data		DIOG 14
MAOP II	2-3.4.2	Descriptive Data		DIOG 14
MAOP II	2-3.5	Indexing Requirements of General Indices Versus Automated Investigative Support Systems		DIOG 14
MAOP II	2-3.6	Responsibilities		DIOG 3 and 14
MAOP II	2-3.6.1	Special Agent		first introductory Paragraph only. DIOG 3
MAOP II	2-3.6.2	Supervisory Special Agent Responsibility		DIOG 14
MAOP II	2-4	Management of Files		DIOG 14
MAOP II	2-4.1	Investigative Files		DIOG 14
MAOP II	2-4.1.1	Serializing		DIOG 14
MAOP II	2-4.1.2	Zero Files		Paragraph (2) only. DIOG 14
MAOP II	2-4.1.3	Double Zero Files		DIOG 14
MAOP II	2-4.1.4	Dead Files - No Pending Investigation		DIOG 14
MAOP II	2-4.1.5	Control Files		Paragraph (1) first four sentences only. DIOG 14
MAOP II	2-4.2	Administrative Files		DIOG 14
MAOP II	2-4.2.1	Noninvestigative Files		DIOG 14
MAOP II	2-4.3.6	Consolidation of Files		DIOG 14
MAOP II	2-4.3.7	Reclassification of Files		DIOG 14
MAOP II	2-5	Case Management - Field Offices		DIOG 14
MAOP II	2-5.1	Opening Cases		Paragraphs 1, 2, 3, 4 (initial paragraph only before sub-letters), 4d, 4e, 4f, and 5 (first sentence only). DIOG various sections
MAOP II	2-5.1.1	Leads		Paragraph (2), delete "Discretionary Action" leads in first sentence only; and delete 2b. DIOG 14
MAOP II	2-5.2	Status of Cases		DIOG 14
MAOP II	2-5.2.1	Pending Case		DIOG 14
MAOP II	2-5.2.2	Pending Inactive		Paragraphs 2, 2a-c, and 3 only. DIOG 14
MAOP II	2-5.2.3	Referred Upon Completion to the Office of Origin (RUC)		DIOG 14
MAOP II	2-5.2.4	Closed		DIOG 6.11, 7.11, 8.8, 9.12
MAOP II	2-5.2.5	Unaddressed Work		DIOG 14
MAOP II	3-1	FBI Classifications/Sub-classifications and Program Groupings		CPD 0015D. RPO/RAU is now responsible for this area by EC 66F-HQ-1079817 serial 705. Link to RPO web-site. Supersede section 3.1 and all subparts.
MAOP II	3-1.1	FBI Classifications and Subdivided Classifications		only 62D; 62E replaced with new 343 classification. 163 M-U classification added. DIOG 12
MAOP II	3-3 (3c)	Task Force Officers (defined)		DIOG 3.3.2
MAOP II	3-3.2 (1)	Special TURK Recording Procedures. (1) Major Cases		#1a-g. DIOG Appendix J-Major Cases
MAOP II	3-4.5 (9 a-g)	Case Count Information (# 9 re: closings)		Paragraph # 9 a-g was superseded by DIOG 6.11; 7.11; 8.8; and 9.12.
MAOP II	3-4.6	Reclassifying Cases and Error Correction		DIOG 6.11.C; 7.11.C; 8.8.C; and 9.12.C

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MAOP II	3-4.8	Criminal Preliminary Inquiries		Paragraph #1 only. DIOG Section 6.7 - PIS are authorized for 6 months; extension authorized for 6 additional months by SAC; and FBIHQ SC; DIOG 14
MAOP II	3-4.10 (1)	Spin-off Cases (paragraph #1 - defined)		DIOG 5, 6, 7, 8, and 9.
MAOP II	3-4.10 (2)	Spin-off Cases (paragraph #2 - who can authorize)		superseded paragraph #1, defined in DIOG 14
MAOP II	3-4.11(1)	Control Files (Paragraph #1 - defined)		superseded paragraph # 2, DIOG 14
MAOP II	3-4.11 (2)	Control Files (Paragraph #2 - leads)		delete third sentence only, DIOG 14
MAOP II	3-4.11 (3)	Control Files (paragraph #3, third sentence only)		DIOG 14.3 (generally)
MAOP II	9	Dissemination of Information		DIOG 14.3, 14.4, 14.5 and 14.6
MAOP II	9-3	Information to Be Disseminated		DIOG 14.3.A and B
MAOP II	9-3 (paragraph 1)			DIOG 14
MAOP II	9-3 (paragraph 2)	AG Memo 9/21/2001 - "Disseminating Information to Enhance Public Safety and National Security."		DIOG 14.3.A.5
MAOP II	9-3 (paragraph 3)			DIOG 14.3.A.3
MAOP II	9-3.1	Dissemination to State and Local Criminal Justice and Noncriminal Justice Agencies		DIOG 14.3
MAOP II	9-3.1.1	Dissemination to State and Local Criminal Justice Agencies		DIOG 14.4.B
MAOP II	9-3.2	Information Totally Within Jurisdiction of Other Federal Agencies		DIOG 3.4.E
MAOP II	9-3.3	Information within FBI Jurisdiction and of interest to another Federal Agency		DIOG 12.4
MAOP II	9-3.4.2	Interested Agency Outside a Field Office Territory		DIOG 12.4
MAOP II	9-3.4.3	Interested Agency Within a Field Office's Territory		DIOG 12.4 and 12.5
MAOP II	9-3.4.4	Reporting Information Furnished		DIOG 12.4 and 12.5
MAOP II	9-3.5	Method of Dissemination to Outside Agencies		DIOG 12 and 14, generally
MAOP II	9-3.5.3	Oral Dissemination to Outside Agencies		DIOG 12.4 and 12.5
MAOP II	9-3.5.4	Accounting of Dissemination		Interview or CHS - DIOG 18.5.6 and CHSPM
MAOP II	9-4.2.6	Investigative Activity in Congressional Offices		Interview or CHS - DIOG 18.5.6. Paragraph (2) Superseded by AGG-Dom, DIOG and AG Memo WH Contacts
MAOP II	9-4.2.9	Dissemination to the White House Complex		DIOG Appendix K - Major Cases
MAOP II	9-6	Major Cases - Dissemination of Information		DIOG 14
MAOP II	9-7	Threat to Life - Dissemination of Information		DIOG 14
MAOP II	9-7.1	Information Concerning Threats Against the President and Other Designated Officials		DIOG 14
MAOP II	9-7.2	Information Concerning Threats, Possible Violence or Demonstrations Against Foreign Establishments or Officials in the US		DIOG 14
MAOP II	9-7.2.1	Information Received Through other Than Technical Surveillance		DIOG 14
MAOP II	9-7.2.2	Information Received Through Technical Surveillance		DIOG 14
MAOP II	9-7.2.3	Miscellaneous		DIOG 14
MAOP II	9-8	Replies to Foreign Police and Intelligence Contacts		DIOG 14
MAOP II	9-8.1	Letterhead Memoranda Prepared by Bureau's Foreign Offices		DIOG 14
MAOP II	9-8.2	Dissemination of Classified Information		DIOG 12 and 14
MAOP II	9-9	Dissemination of Grand Jury Material		DIOG 18.6.5
MAOP II	9-10	Dissemination of Title XI, Right to Financial Privacy Act of 1978		DIOG Appendix O - RFPA
MAOP II	9-13	Dissemination By Field Intelligence Groups		DIOG 14
MAOP II	10-9	General Rules Regarding Recording and Notification of Investigations		Supersede Paragraphs # 1a-c; 2a-c; 5; 6; 7; 9; 10a-c; 11-16; and 23-24, DIOG, various sections.
MAOP II	10-10.9.1	Approval by individuals Delegated to Act on Behalf of Higher Bureau Officials		DIOG 3.4.C
MAOP II	10-12	Notes made During Investigations - Interviews		DIOG 3 and 14
MAOP II	10-16.2	Office of Origin		DIOG 14

UNCLASSIFIED//FOUO
DIOG Supersessions

Part	Section	Section Title	DIOG 1 Supersession	DIOG 2 Supersession
MAOP II	21-7 (6)	Monitoring, Documenting and Reviewing		Remove second to last and last sentence only. Remove citation to MAOP at the end of Paragraph # 6 and add citation "See DIOG 3.4.D"
NA	EC	319T-HQ-A1487667-INSO, ser. 247		34.D
N/A	EC	To Provide Guidance on Least Intrusive Techniques in National Security and Criminal Investigations - OGC EC (319X-HQ-A1487720-OGC Serial 1), 12/20/2007	DIOG 4, 4.1, 11.1.1	DIOG 4, 4.4, 18.1.1-2
N/A	EC	Mail Cover Cites - EC dated 12/22/2004	DIOG 11.3	DIOG 18.6.10
MIOG II	10-10.17.1	FD-670, Consensual Monitoring - Telephone Checklist	DIOG 11.5	DIOG 18.6.1
N/A	form	FD-671, Consensual Monitoring - Non-telephone Checklist	DIOG 11.5	DIOG 18.6.1
N/A	EC	Electronic Surveillance - EC dated 12/20/2007	DIOG 11.12	DIOG 18.7.2-3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 3/19/2004		DIOG 4.1, 6.3, 8.3, 9.3, 15.3
N/A	EC	Civil Liberties and Privacy EC issued by OGC dated 9/8/2005		DIOG 4.1, 7.3
N/A	EC	Least Intrusive Techniques in National Security and Criminal Investigations - EC issued by OGC on 12/20/2007, file number 319X-HQ-A1487720-OGC-		DIOG 4, 4.4, 18.1.1-2
N/A	EC	Protection of First Amendment Rights EC issued by OGC dated 3/19/2004 EC issued by CTD dated 09/01/2004 EC issued by OGC dated 12/05/2003		DIOG 4.2
N/A	EC	FBI National Collection Requirements EC issued by DO dated 01/30/2003		DIOG 5.11
N/A	EC	Retention and Dissemination of Privacy Act Records EC issued by OGC dated 03/19/2004		DIOG 5.13
N/A	EC	Authorized Investigative Methods in Assessments ECs issued by OGC dated 03/19/2004 and 9/18/2005		DIOG 18.3, 18.5
N/A	EC	Authorized Investigative Methods in Full Investigations EC issued by OGC dated 10/29/2003		DIOG 18.3, 18.7
N/A	EC	Federal Grand Jury Subpoena EC issued by OGC dated 06/01/2007		DIOG 18.5.9, 18.6.5
N/A	EC	Administrative Subpoena EC issued by CID dated 06/06/2001		DIOG 18.6.4
N/A	EC	Voluntary Disclosure of Non-Content Customer Records		DIOG 18.6.8
N/A	EC	Definition of Investigative Method EC issued by OGC dated 10/14/2003		DIOG 18.6.9.3
N/A	EC	FISA Review Board for RISA Renewals EC issued by Director's Office dated 02/06/2006		DIOG 18.7.3.1.5.3
N/A	EC	Assistance to Other Agencies EC issued by OGC dated 12/5/2003		DIOG 12
N/A	EC	Emergency Disclosure Provision for Information from Service Providers Under 18 U.S.C. Section 2702(b) - EC issued by OGC 08/25/2005, file number 66F-HQ-1085159 and 66F-HQ-C1364260		DIOG 18
LHSA	7-4.1(7)	Consolidated Legal Handbook for Special Agents Section 7-4.1(7) into Interview Section of DIOG		DIOG 18
N/A	EC	Electronic Recording of Confessions and Witness Interviews -EC issued by OGC on 03/23/2006, file number 66F-HQ-1233488-3 and 66F-HQ-C1384970.		DIOG 18
N/A	EC	FBI Mandated File Review Process - EC issued by INSD on 07/07/2010, file number 319T-HQ-A1487667-INSO-247		DIOG 3
N/A	EC	Electronic Recording of Confessions and Witness Interviews - EC issued by OGC on 03/23/2006, file numbers 66F-HQ-C1384970 and 66F-HQ-1233488		DIOG 18
N/A	EC	Procedural and Operational Issuance - Guidance for Legislative Corruption - EC issued by CID on 08/08/2006, file number 319W-HQ-A1487699-CID-253		DIOG 18
N/A	EAU EAP PG	FBI Employee Assistance Unit, Employee Assistance Program PG, delete definition of task force officer on page 1		DIOG 3
N/A	RAP Tool User Guide v1.1	Resource Allocation Planning (RAP) Tool, User Guide v1.1 - delete definition of task force officer and task force member on page 1		DIOG 3

APPENDIX S: (U) LISTS OF INVESTIGATIVE METHODS

S.1 INVESTIGATIVE METHODS LISTED BY NAME (ALPHABETIZED)

- (U) Administrative subpoenas. (Section [18.6.4](#))
- (U) CHS use and recruitment. (Section [18.5.5](#))
- (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices. (Section [18.6.3](#))
- (U) Consensual monitoring of communications, including electronic communications. (Section [18.6.1](#))
- (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information). (Section [18.7.3](#))
- (U) Electronic surveillance – Title III. (Section [18.7.2](#))
- (U) FISA Order for business records. (Section [18.6.7](#))
- (U) Grand jury subpoenas. (Section [18.6.5](#))
- (U) Grand jury subpoenas – only for telephone or electronic mail subscriber information in Type 1 & 2 Assessments. (Section [18.5.9](#))
- (U) Information voluntarily provided by governmental or private entities. (Section [18.5.7](#))
- (U) Intercepting the communications of a computer trespasser. (Section [18.6.2](#))
- (U) Interview or request information from the public or private entities. (Section [18.5.6](#))
- (U) Mail covers. (Section [18.6.10](#))
- (U) National Security Letters. (Section [18.6.6](#))
- (U) On-line services and resources. (Section [18.5.4](#))
- (U) Pen registers and trap/trace devices. (Section [18.6.9](#))
- (U) Physical Surveillance (not requiring a court order). (Section [18.5.8](#))
- (U) Polygraph examinations. (Section [18.6.11](#))
- (U) Public information. (Section [18.5.1](#))
- (U) Records or information - FBI and DOJ. (Section [18.5.2](#))
- (U) Records or information - Other federal, state, local, tribal, or foreign government agency. (Section [18.5.3](#))
- (U) Searches – with a warrant or court order. (Section [18.7.1](#))

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

(U) Stored wire and electronic communications and transactional records. (Section 18.6.8)

(U) Trash Covers (Searches that do not require a warrant or court order). (Section 18.6.12)

(U) Undercover Operations (Section 18.6.13)

S.2 INVESTIGATIVE METHODS LISTED BY ORDER IN DIOG SECTION 18

18.5.1 (U) Public information

18.5.2 (U) Records or information - FBI and DOJ.

18.5.3 (U) Records or information - Other federal, state, local, tribal, or foreign government agency.

18.5.4 (U) On-line services and resources.

18.5.5 (U) CHS use and recruitment.

18.5.6 (U) Interview or request information from the public or private entities.

18.5.7 (U) Information voluntarily provided by governmental or private entities.

18.5.8 (U) Physical Surveillance (not requiring a court order).

18.5.9 (U) Grand jury subpoenas – only for telephone or electronic mail subscriber information.

18.6.1 (U) Consensual monitoring of communications, including electronic communications.

18.6.2 (U) Intercepting the communications of a computer trespasser.

18.6.3 (U) Closed-circuit television/video surveillance, direction finders, and other monitoring devices.

18.6.4 (U) Administrative subpoenas.

18.6.5 (U) Grand jury subpoenas.

18.6.6 (U) National Security Letters.

18.6.7 (U) FISA Order for business records.

18.6.8 (U) Stored wire and electronic communications and transactional records.

18.6.9 (U) Pen registers and trap/trace devices.

18.6.10 (U) Mail covers.

18.6.11 (U) Polygraph examinations.

18.6.12 (U) Trash Covers (Searches that do not require a warrant or court order).

18.6.13 (U) Undercover operations.

UNCLASSIFIED – FOR OFFICIAL USE ONLY
Domestic Investigations and Operations Guide

18.7.1 (U) Searches – with a warrant or court order.

18.7.2 (U) Electronic surveillance – Title III

18.7.3 (U) Electronic surveillance – FISA and FISA Title VII (acquisition of foreign intelligence information).

UNCLASSIFIED//FOUO



**DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE
INVESTIGATIVE METHODS AND APPROVAL CHARTS**

OCTOBER 16, 2013

UNCLASSIFIED//FOUO

Undisclosed Participation (UDP) Approval Levels for Assessments and Predicated Investigations* (dated 10/16/2013)
(All CHS tasking must be in conformity with FBI CHS policy)

CHS or UCE Status	Non-Sensitive UDP			Sensitive UDP	
	Using a CHS or UCE for:			Using a CHS or UCE for:	
	Obtain information	Intended or likely to influence the activities of an organization	Intended or likely to influence the exercise of 1st Amendment rights by members of the organization	Obtain information	Intended or likely to influence the activities of an organization or the exercise of 1st Amendment rights by members of the organization
CHS already a member of the organization and is tasked to obtain information	Assessments: SSA approval required; UCE role not permitted.	Assessments: Not permitted.	Assessments: Not permitted.	Assessments: SSA approval. If obtaining information not generally known to regular members ("insider information"), CDC review and SAC approval. UCE role not permitted.	Assessments: Not permitted.
CHS or UCE not currently a member; tasked to join/participate and obtain information	Predicated Investigations: No supervisory approval required for CHS activity. Employee's role requires SSA approval. UCE role requires SSA approval or higher. UCO policy may apply.	Predicated Investigations: CDC review and SAC approval. UCO policy may apply.	Predicated Investigations: OGC review. If OGC determines participation: (1) will or is likely to influence exercise of 1st Amendment rights of members of the organization, EAD or higher approval, and notice to SORC required; or (2) will not likely influence the exercise of First Amendment rights, AD may approve with notice to SORC. UCO policy may apply.	Predicated Investigations: SSA approval.	Predicated Investigations: OGC review. If OGC determines participation: (1) will or is likely to influence the activities of the organization, but not likely influence the exercise of First Amendment rights, AD may approve with notice to SORC. (2) will or is likely to influence exercise of 1st Amendment rights by members of the organization, OGC and SORC review and Director approval; or (3) will not likely influence either the activities of the organization nor the exercise of 1st Amendment rights, UDP request returned to Field Office for requisite UDP approval.
Special Rules for Attending Religious Services and Other Sensitive Organizations (EOG Sections 18.5.1.3.1, 18.5.5.5 (C) and (D))					

Definitions & Notes:

Definition of Sensitive UDP:

Sensitive UDP is the activity of a political, religious, or media organization, an academic institution, an organization having an academic focus, or an organization whose primary purpose is the advocacy of social or political causes or the education of the public about such issues.

1. "In frequent attendance" (3 times or less) by a person does not constitute "participation," but, tasking a CHS to attend or having an agent attend, does require approval.

In Assessments:

- a) Religious Services –
 - i. Tasking a CHS to attend: SAC approval (non-delegable).
 - ii. Employee's overt attendance: SSA approval.
 - iii. UCE attendance: not allowed.
- b) Other Sensitive Organizations –
 - i. Tasking a CHS to attend (other than a public gathering of a substantial number of non-members): SSA approval.
 - ii. Employee's overt attendance: no approval required.

In Predicated Investigations:

- a) Religious Services –
 - i. Tasking a CHS to attend: SSA approval.
 - ii. Employee's overt attendance: SSA approval.
 - iii. UCE attendance: see UCO policy.
 - b) Other Sensitive Organizations – no approval required.
2. Tasking a CHS to attend or an employee's overt attendance of more than 3 times in any of these organizations will be treated as "participation" for purposes of the UDP policy.

Exclusions for UDP approval DO NOT apply in any of the following circumstances:

1. Information is voluntarily provided by a CHS who is already a member of an organization or joins on his or her own behalf (not tasked).
2. Information is derived from attending events or activities that are open to the general public and obtained on the same terms and conditions as members of the general public.
3. Organization is openly acknowledged by a foreign government to be directed or sponsored by that foreign government.
4. Organization is reasonably believed to be acting on behalf of a foreign power and its U.S.-based membership consists primarily of non-US Persons.
5. Organization was not formed for a lawful purpose or its primary purpose is to engage in unlawful activities.

Methods of Analysis for UDP:

1. Is there an Organization?
2. Is the Organization legitimate or real?
3. Is it a U.S. or Foreign Organization?
4. Is it then sensitive or Sensitive UDP?
5. Assessment or Predicated Investigation?
6. Has participation been recognized by an appropriate official?
7. Is CHS already member/participant or CHS/UC: tasked to participate?
8. What is the purpose: tasked to obtain info / influence activities / influence 1st Amend / attend religious service?

Field Office Investigations Chart (Date 10/16/2013)

Assessments									
Investigation	Purpose	Duration	Documentation	Opening Approval	Closing Approval	Justification Review	EC	Responsible Entity	Notification
Type 1 & 2 Assessments	Seek information, proactively or in response to investigative leads, relating to activities – or the involvement or role of individuals, groups, or organizations in these activities – constituting violations of federal criminal law or threats to the national security	As long as necessary to achieve purpose and objective. No time limit	FD-714 or Guardian (as soon as practical). When not converted to Protected Investigation, it must be converted to have an assessment file, already open matter, and/or recent work file	Any employee can open; SSA or SA design	No notice required	Every 30 days	CDC review, SAC approval, as soon as practicable, but not more than five (5) business days	FO investigative squad or FBIHQ operational division	No notice to FBIHQ or DOJ required when opening or closing
Type 3 Assessment	Identify, obtain and utilize information about actual or potential national security threats or federal criminal activities, or the vulnerability to such threats or activities	As long as necessary to achieve purpose and objective. No time limit	Opened with EC, FD-707, 607 or 615 classification; FO squad or FBIHQ operational division - investigative file classification	Prior written SSA or SA approval (No oral approval)	Closed with an EC approved by SSA or SA	Every 30 days, if probationary employee, every 60 days	CDC review, SAC approval, as soon as practicable, but not more than five (5) business days	FIG, CI or CI unit, FO investigative squad, FBIHQ operational division	No notice to FBIHQ or DOJ required when opening or closing
Type 4 Assessment	Obtain and retain information to obtain or facilitate intelligence analysis and reporting	As long as necessary to achieve purpose and objective. No time limit	Opened with EC only by FIG, 615A-F or 615H classification	Prior written SSA (FIG) or SA approval (No oral approval)	Closed with an EC approved by SSA (FIG) or SA	Every 30 days, if probationary employee, every 60 days	CDC review, SAC approval, as soon as practicable, but not more than five (5) business days	FIG, FIGS, or FBIHQ Ops Division Unit Component	No notice to FBIHQ or DOJ required when opening or closing
Type 5 Assessment	Seek information to identify potential human sources, assess their suitability, reliability, or value of individuals as human sources	As long as necessary to achieve purpose and objective. No time limit	Opened with EC or successor Delta form; 615H, 615T or 615R classification	Prior SA, (prior written approval from SSA, for SA, prior written approval from both the SA and the SSA of the investigation or HUMINT asset that will potentially recruit the individual. (No oral approval)	Closed with an EC (or successor form in Delta form by SSA) or SA who were required to open	Every 30 days, if probationary employee, every 60 days	See DIOG for sensitive potential CHS or Group	FO, SA or SA assigned to investigative squad or the FIG, FBIHQ, SA	No notice to FBIHQ or DOJ required when opening or closing
Type 6 Assessment	Seek information, proactively or in response to investigative leads, relating to matters of foreign intelligence interest responsive to foreign intelligence requirements	As long as necessary to achieve purpose and objective. No time limit	Opened with EC only by FIG, 609-614 or 615 classification; incidental collection - 615 classification	Prior written SSA or SA, (No COMULC approval - No oral approval)	Closed or converted to a Full Investigation with an EC approved by the SSA (FIG) or SA, and the responsible CI UC	Every 30 days, if probationary employee, every 60 days	CDC review, SAC approval, and the responsible CI UC as soon as practicable, but not more than five (5) business days	FIG, SA or SA (investigative squad can support)	Notice to CI with request to open EC; No notice required to DOJ of opening or closing
This chart will be updated for Type 1 & 2 Assessments and Type 3 Assessments to include the documentation of investigative requirements									
Predicated Investigations									
Investigation	Predication	Duration	Documentation	Approval to Open	Closing Approval	File Review	SA	Responsible Entity	Notification
Preliminary Investigation (PI)	"Information or an allegation" indicating the existence of federal criminal activity or a threat to national security (or predicated against such activity or threat) See DIOG 5.5	6 months, One (6) month extension with SAC approval; defensible to AGAC. Additional 6 month extensions by responsible FBIHQ Section Chief (for "good cause")	EC	Prior written SSA Approval. Oral SSA approval permitted, but must be documented within 5 business days. See DIOG 3.4.2.2 and 6.7.1	SSA approval. Closing a SIM requires SAC approval	Every 30 days, if probationary employee, every 60 days	CDC Review and SAC Approval as soon as practicable, but not more than five (5) business days, within notice to the appropriate FBIHQ operational UC and SC within 15 calendar days. FO or FBIHQ must notify USAO unless inappropriate; FBIHQ must notify DOJ	Investigative Squad	Opened or Closed by FO - no notice to FBIHQ (PIs may require notice); USAO or DOJ, unless PI is a SIM. USAM, FO notifies FBIHQ Unit and Section, and USAO, if appropriate. Opened or Closed by FBIHQ - notice to applicable FOs, DIOG 4.7.1 and 6.12.2
Full Investigation	"Articulable factual basis" that reasonably indicates the existence of federal criminal activity or a threat to national security (or predicated against such activity or threat) or obtain foreign intelligence responsive to a PFI Collection Requirement. See DIOG 7.5	No time limit, as long as articulable predication continues to exist	EC	Prior written SSA Approval. Oral SSA approval permitted, but must be documented within 5 business days. See DIOG 3.4.2.2 and 6.7.1	SSA approval. Closing a SIM requires SAC approval	Every 30 days, if probationary employee, every 60 days	CDC Review and SAC Approval as soon as practicable, but not more than five (5) business days, within notice to the appropriate FBIHQ operational UC and SC within 15 calendar days. FO or FBIHQ must notify USAO unless inappropriate; FBIHQ must notify DOJ within 30 calendar days	Investigative Squad	Opened by FO - notice to responsible FBIHQ Unit within 15 calendar days. Closed by FBIHQ notice to applicable FO within 15 calendar days. National security investigations of USPCRS require FBIHQ notice to DOJ/NSD within 30 calendar days. Closed by FO - no notice to FBIHQ or DOJ is required; PFI may require notice, unless it is a SIM. If SIM, notice to operational FBIHQ Unit and Section, and to the USAO, if appropriate. Opened or Closed by FBIHQ - notice to applicable FOs. See DIOG 7.5
Enterprise Full Investigation	"Articulable factual basis" for the investigation that reasonably indicates the group or organization is or may be engaged in Risk-Raising, IT, or DT activities. See DIOG 3.4	No time limit, as long as articulable predication continues to exist	EC	Prior written FBIHQ SC approval. One SC approval permitted, but must be documented within 5 business days. See DIOG 3.4.2.2 and 6.6.1	SAC and appropriate SC approval	Every 30 days, if probationary employee, every 60 days	CDC Review, SAC and SC Approval, as soon as practicable, but not more than five (5) business days, within notice to the appropriate FBIHQ operational UC and SC within 15 calendar days. FO or FBIHQ must notify USAO, if appropriate. FBIHQ must notify DOJ within 30 calendar days	Investigative Squad	FBIHQ Section receives notice with the opening EC. Responsible FBIHQ Section must notify DOJ (NSD or OCSG) within 30 calendar days. If SIM, notice must be given to USAO, if appropriate.
PFI/CI Investigation	Investigation may obtain foreign intelligence that is responsive to a Positive Foreign Intelligence Collection Requirement	No time limit, until the PFI Collection Requirement is satisfied	EC	Prior written approval from the responsible CI UC (oral approval not permitted)	Responsible CI Unit, Closing a SIM requires SAC (if opened in the field) and responsible CI SC approval	Every 30 days, if probationary employee, every 60 days	CDC Review, SSA, SAC and CI SC approval, as soon as practicable, but not more than five (5) business days. CI must notify DOJ/NSD within 30 calendar days	FIG	CI must notify DOJ/NSD within 30 calendar days

Investigative Methods Approval Chart (dated 10/16/2015)

[illegible]